



# Securing Your Network and Application Infrastructure

24 Experts Share Their Secrets



SPONSORED BY:

**FORTINET**

# TABLE OF CONTENTS

Foreword .....	3	True Security Requires Understanding and a Layered Security Approach.....	31
Introduction .....	4		
<b>Building and Executing a Plan for Your Network Security</b>		<b>Staying Ahead of Hackers</b>	
Cover the Basics.....	6	Becoming Proactive.....	34
Strengthening Information Security: A Long-Term Process.....	8	What Keeps Me up at Night.....	36
Security Must Be Easy.....	10	Hunting the Hunters.....	38
Greatest Challenges: Speed and Complexity.....	12	<b>Protecting Against APTs and Application-based Attacks</b>	
Too Many Solutions, Not Enough Answers.....	14	Applications Represent Today's Greatest Security Risks.....	41
The Five Key Points for Securing Your Network and Application Infrastructure.....	16	Delayed Threat Detection and Slow Response Pose the Greatest Threats.....	43
Making the Business Case for Stronger Security.....	18	<b>The Human Factor and a Culture of Security</b>	
Don't Forget the Basics.....	20	Security Is a Technical and a Human Problem.....	46
<b>Protecting the Core of Your Network</b>		Even Great Firewalls Can be Compromised.....	48
Managing Vendor Security Is Critical to Our Business.....	23	Communication and Culture.....	50
Securing Vital Data Is the Greatest Challenge.....	25	Effective Information Security Requires Thorough User Education.....	53
The Disappearance of the Perimeter Is the Greatest Security Challenge.....	27	People, Technology, and Security.....	55
Closer to the Heart.....	29	Social Security.....	58

# FOREWORD

Network security challenges are evolving faster than ever as a result of new technologies and application complexity. In addition, many old issues continue to plague organizations, from simple password security to keeping software up-to-date.

This collection of 24 essays covers a broad array of topics grouped into five major areas, ranging from the necessity of planning your network security up front to the new challenges that social engineering and other advanced, persistent threats bring. A major theme throughout many of them is the loss of the perimeter and the effectiveness of traditional defenses. Bring Your Own Device (BYOD) and cloud-based services open many holes in an organization's network that require a rethinking of security to protect the data themselves, not just the methods of accessing it.

Fortinet's Cyber Security platform can address most of the problems outlined in the essays in this e-book. Our ASIC-powered FortiGate firewalls deliver the industry's fastest Next Generation Firewall (NGFW) performance and are the foundation of an end-to-end security solution that spans your users, network, data centers, and the cloud. For the problems we can't solve directly, we offer tools such as enforcing business policies on password changes and vulnerability scanners for your applications to help you catch weaknesses.

We hope you find these essays as interesting and thought provoking as we do and that they can help you improve your network and application security defenses.



## **Advanced Cybersecurity from the Inside Out**

Fortinet is a global leader and innovator, providing an integrated platform of high-performance, cybersecurity solutions that span from the datacenter to the cloud — serving small, medium and enterprise organizations around the globe.

Strengthened by the industry's highest level of real-time threat intelligence and recognized with unparalleled third party certifications, Fortinet solves the most important security challenges of more than 210,000 organizations. Trust Fortinet to take care of security so you can take care of business.

[Learn more at fortinet.com](https://www.fortinet.com)

# INTRODUCTION

For all the attention data security has received in recent years and all the technical advances in risk detection now available to protect network infrastructures, you might imagine that data are safer than ever before. Unfortunately, the number of recent, frighteningly large data breaches contradicts that notion. In the past 18 months alone, we have seen breaches at Adobe, eBay, JPMorgan Chase, Target, Home Depot, Community Health Services, and the US Government that together compromised more than 500 million records. Will the world ever be a safe place for the data so vital to businesses and individuals?

With the generous support of Fortinet, we have created this e-book to help you better understand the security challenges that business—and mid-sized businesses in particular—face today. This e-book is a compilation of responses to the following question:

## ***What are the greatest challenges you face in securing your network and application infrastructure?***

A range of industry analysts, consultants, and hands-on security experts provided responses to this question. They offered fascinating insights into the security challenges we face today—security issues made even more challenging because of the changing character of infrastructure and its loss of network perimeter, rapidly evolving application environment, lack of security awareness among users, and the increasing complexity of security solutions. Attacks and data theft have also become a big business underwritten by sophisticated, well-funded entities.

Security and vigilance are a never-ending battle, but I trust you will find the many perspectives provided by those who are on the front lines useful as you work to secure your own business infrastructures.



All the best,  
**David Rogelberg**  
Publisher



### **Mighty Guides make you stronger.**

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

© 2015 Mighty Guides, Inc. | 62 Nassau Drive | Great Neck, NY 11021 | 516-360-2622 | [www.mightyguides.com](http://www.mightyguides.com)

# In cybersecurity, there's **A LOT OF HYPE...**

**...and then there are facts.**

**Flashy marketing** has a way of clouding the truth: slow is broken. You don't have to choose between having a strong security posture and having optimal network performance to power your business.

**You can have both – but only from us.**

Get a Cyber Threat Assessment today and get the facts about your security posture.

[www.fortinet.com/ctap](http://www.fortinet.com/ctap)

**FORTINET®**

**99%** effective breach detection

**5X NGFW** performance

**#1 unit share** worldwide in network security

**Over 200** zero-day attacks discovered



Data Center Firewall  
Next Generation Firewall  
Breach Detection  
Web Application Firewall

Security Without Compromise

# Building and Executing a Plan for Your Network Security

In this Section...

---



**Shawn E. Tuma**  
Scheef & Stone, LLP.....6



**Patrick Peterson**  
Agari.....14



**Eric Vanderburg**  
Cybersecurity Investigator.....8



**Dan Twing**  
EMA.....16



**Russell Rothstein**  
IT Central Station.....10



**David Harley**  
ESET.....18



**Nigel Fortlage**  
GHY International.....12



**Ryan Dewhurst**  
Dewhurst Security.....20



**SHAWN  
E. TUMA**

Partner,  
Scheef & Stone, LLP

Shawn Tuma is a lawyer who helps business leaders solve problems with cutting-edge issues involving cybersecurity, data privacy, and computer fraud. Specializing in intellectual property law and litigation, Shawn is a frequent author and speaker on these issues. He is a partner at Scheef & Stone, LLP, a full-service commercial law firm in Texas that represents businesses of all sizes throughout the United States and, through its Mackrell International network, the world.

 |  | 

Earlier this year, a restaurant group in my hometown had a payment card breach. In response, the group members committed the cardinal sin: they panicked.

Before the company completed its internal investigation, someone took to its Facebook page and announced the breach, apparently trying to put a positive public relations spin on it. Bad idea. The company impulsively jumped out front of a data breach through social media before compiling enough information to tell the whole story. Predictably, the community rebelled. That was as much a failure of planning as of public relations.

As an attorney, my role is to serve as a breach guide. To that end, I work with a lot of the sorts of people reading this e-book.

Thoroughly understand the data your organization has on hand: that's always my first piece of advice to business leaders. You can't protect what you don't even know exists, so be sure to catalog and classify all of your company's data according to defined criteria.

Next, I ask my clients to assess all threat vectors and external access points. This is an important point: it's not all about your employees. If third parties have access to the corporate network, they may represent a major security weakness (recall that the massive Target Corp. breach in 2013 resulted from bad guys hacking into a small refrigeration systems contractor that had access to Target's network). You might need to impose tight restrictions on third party business partners' access to your corporate network.

*“Thoroughly understand the data your organization has on hand. You can't protect what you don't even know exists.”*

## KEY LESSONS

- 1 THOROUGHLY CATALOG ALL YOUR DATA, REVIEW THE ACCESS THAT THIRD PARTIES HAVE TO YOUR NETWORK, AND PUT AUTOMATED SECURITY TOOLS IN PLACE.
- 2 A THREAT AND BREACH RESPONSE PLAN IS BECOMING A LEGAL ESSENTIAL.





# COVER THE BASICS

Third, inventory your security investments with a focus on automated systems. The organization must have an effective firewall, reputable antivirus software, and both intrusion-detection and intrusion-prevention systems. These technologies can automatically block most known threats. When these systems detect an intrusion, they trigger alerts so that the organization can take appropriate defensive action. Automated security tools not only help keep malicious hackers at bay but, because they can help monitor data flowing in and out of the corporate environment, more accurately help your organization maintain and track its data.

Finally, draw up a breach response plan. It will specify whom the systems alert, a list that should include:

- Legal counsel;
- Digital forensics investigators; and
- An internal data breach management team, consisting of the chief information officer, chief information security officer, public relations, the chief executive officer, and possibly the chief financial officer.

Having a breach response plan in place isn't just good practice internally; it's rapidly becoming a legal essential. By now, most companies either have been breached or are being targeted. Regulators get that. What they don't understand—and certainly won't like—is when attackers penetrate your company without your having a plan in place to protect your customers' data and respond effectively to the breach. Failure along these lines could spell real trouble for your company.

If there's a moral to this story, it's this: cover the basics.

“

*By now, most companies either have been breached or are being targeted.*

”



# STRENGTHENING INFORMATION SECURITY: A LONG-TERM PROCESS



**ERIC  
VANDERBURG**

Security Executive, Author,  
Cybersecurity Investigator,  
and Expert Witness

Eric Vanderburg has been called the *Sheriff of the Internet* for his diligent work in protecting companies and the public from cyber threats. He consults and writes on information management, storage networking, cybersecurity, and risk management. His articles have appeared in major magazines and been translated into many languages. Eric makes regular appearances at conferences and speaks on a variety of security topics on radio and television.

    
Twitter | Website | Blog

Securing your network and application infrastructure is a long-term process. When choosing the right network security appliances and application security solutions, your company must first understand its needs, including the confidentiality or sensitivity level of the data you have, where the data are currently located and where they will be in the future, how the data are accessed, and how accessible the data must be. From this, your organization can create a list of requirements and high-level specifications for the solution.

Next, assess the cost associated with the disclosure of sensitive information or the loss of access to important information, and create a budget for the solution that reasonably mitigates the risk. These two elements allow for informed decision making and aid in the proper implementation of the solution. From the requirements and cost factors, you can create success metrics.

Having the right network security appliances and application security solutions are important, as well, but of course they are not the whole solution. Network security controls should automatically enforce technical elements of a security policy, such as password complexity, authentication, authorization, system monitoring and alerting, packet screening, access control lists, and much more. In addition, the people who use the system must be trained and competent in performing their tasks. You must properly design, enforce, and audit the procedures and policies that define the actions to be taken.

“ When choosing the right network security appliances and application security solutions, your company must first understand its needs. ”

## KEY LESSONS

- 1** STRENGTHENING INFORMATION SECURITY IS A LONG-TERM PROCESS AND MUST INCLUDE OPERATIONS, HUMAN RESOURCES, FINANCE, AND MANY OTHER UNITS IN ADDITION TO THE IT DEPARTMENT.
- 2** IT'S IMPORTANT TO IDENTIFY THE RIGHT TECHNOLOGY SOLUTION FOR YOUR SECURITY NEEDS, BUT THE HUMAN ELEMENT IS EQUALLY CRITICAL.



# STRENGTHENING INFORMATION SECURITY: A LONG-TERM PROCESS

When these parts are all in place, they make for a secure solution that is integrated into rather than ancillary to the business.

Here's an example of what can go wrong when you neglect the human aspect of information security as part of the planning process. I once worked with a company that was outsourcing operations to business associates. A physician was transcribing her notes about a patient, and the transcription service that she used was outsourced two levels deep: once to the company handling the transcriptions, and then again to a company handling the data storage for those transcriptions. Somebody at the data storage firm stored the data in the wrong location, and then private information about a patient was suddenly available in Google search results. Had this company had effective vendor controls in place, it could have avoided compromising the patient's private data.

Implementing strong security measures takes time and effort. If your company is not at the bar and you have to get to that bar, you're going to have to take baby steps. You can't do it all in a weekend or even in a month. Figuring out how to effectively plan that long-term approach is essential.

“

*Had this company had effective vendor controls in place, it could have avoided compromising the patient's private data.*

”

# SECURITY MUST BE EASY



**RUSSELL  
ROTHSTEIN**  
CEO and Founder,  
IT Central Station

Russell Rothstein is the founder and CEO of IT Central Station, the leading crowd-sourced product review site for InfoSec and other enterprise software. Before founding IT Central Station, Russell worked for 20 years in enterprise tech companies such as OPNET, Nolio (bought by CA), and Oracle. Russell received a B.A. degree in computer science from Harvard University, an M.S. degree in technology and policy from MIT, and an M.S. degree in management from the MIT Sloan School of Management.

    
Twitter | Website | Blog

On my site, I often see buyers looking for solutions to eliminate their security challenges. Some of the biggest challenges they face when they're securing their networks and application infrastructure are visibility, ease of use, stability, and reliability.

First and foremost, traffic visibility is an important issue that buyers must address and the biggest challenge users face. If you don't see what's going on, then small threats can become major issues. For example, data breaches have recently been in the news—the U.S. Office of Personnel Management and Harvard University are two well-known instances. Those data breaches were potentially traffic visibility issues.

A common question I see is, how do you get that clear visibility into traffic in the environment, on the network, and in the applications? People want full visibility because it enables them to go from being terrified about protecting the environment to being in full control. A good firewall can keep your private information secure while being easy to use and not too burdensome. IT Central Station recently announced the top 10 enterprise firewalls based on data from more than 85,000 views from 2014 to the first quarter of 2015: Fortinet FortiGate came out as the leader.

Ease of use and reporting features are also real challenges. I often hear from users that they wish the user interface (UI) were easier to understand. People mention that with FortiGate, for example, adding troubleshooting and network testing features to the UI would be useful.

“If you don't see what's going on, then small threats become major issues.”



## KEY LESSONS

- 1 GAINING CLEAR VISIBILITY INTO THE TRAFFIC ON YOUR NETWORK IS AN ESSENTIAL ELEMENT FOR PROTECTING THE ORGANIZATION.
- 2 NOT ALL THE FEATURES OFFERED IN SECURITY PRODUCTS ARE NECESSARY. DON'T GET CAUGHT UP IN THE BELLS AND WHISTLES; INSTEAD, FOCUS ON THE FEATURES YOU REALLY NEED.

# SECURITY MUST BE EASY

People also tell me they can't read configuration files without third-party tools. Reporting isn't seamless, and for some, it takes too much work to manage and determine what's going on with their system. Although difficult, reporting must be easy to use, clear, and intuitive. When it's not, problems occur. It's just like an alarm in your house. If it's a pain to set, you won't use it consistently. If it's easy to set, then when you walk out the door, you'll set it and know that your home is protected when no one's there.

It's not just the software, either. Many individuals aren't clear on which product features are best for their companies, and the tendency of vendors to add hardware to devices can make this decision even more difficult. Understanding whether clustering, link aggregation, port sensitivity, or all of these are needed for your situation can be difficult to determine. Professionals don't always have the time to become experts in every product they purchase; instead, they often rely on peer recommendations and reviews to determine which features they need.

The software and hardware are the basic components of security solutions, but being able to navigate the features you need is also necessary. Having a single administrative interface is extremely important, because most organizations have a patchwork of security products. That means more dashboards, more interfaces, and more reports are getting all this data coming at different times, making it more difficult to manage and control your network. So, having a pane of glass—a single administrative interface or graphical UI that connects them all and is easy to use—is critical.

Stability is another challenge, although less prominent than the others. Finding stability in an information security system that scales; is reliable; doesn't crash; and works in a multivendor, heterogeneous environment is difficult. All those things are important, especially now, in a world of Bring Your Own Device, where so much data are accessible through a mobile device. It's vital that whatever security measures are in place will support all these platforms and "just work."

Fortunately, you're not alone in overcoming these challenges. Crowd-sourced review sites like IT Central Station create an unbiased community of professionals who have already done the research and built best practices so you don't need to reinvent the wheel. Sites like ours help to keep you informed so that you can make the best decisions about the right security solutions for your organization.

“

*Having a pane of glass—a single administrative interface or graphical UI that connects them all and is easy to use—is critical.*

”

# GREATEST CHALLENGES: SPEED AND COMPLEXITY



**NIGEL  
FORTLAGE**

Vice President, IT,  
GHY International

Nigel Fortlage is a diverse leader, overseeing all aspects of social media, participating on executive and business development teams, and the senior executive in charge of IT. Nigel has a certificate in applied management through the University of Manitoba and is a recipient of the prestigious IBM Innovation award. He also shares his passion, knowledge, and insights through articles, interviews, and public speaking both nationally and internationally. Nigel is a founding member of the CIO Association of Canada and president of its Manitoba chapter; in 2014 and 2015, *Huffington Post* named him in the Top 100 Most Social CIOs on Twitter.

 |  |   
Twitter | Website | Blog

When I first met the members of our new board of directors, one of their questions was about data security. In my role as chief information officer, I spend a lot of time thinking about how best to secure my company's data. From my perspective, the two greatest security challenges we face are:

- The speed, frequency, and variation of attacks and how quickly they change; and
- The complexity of the network infrastructure, which consists of diverse channels and resources that include on-premises systems, off-premises services, and public networks.

People often think that the sensitive business data—financial information, trade secrets, personal information—must have the strongest protection. Of course, those data are critical, but other valuable data assets must also be protected. For instance, part of my role involves social networking outreach, and one question we must answer is how to protect our online content assets, including video and images. In our sharing culture, it is nearly impossible to prevent others from picking up and using those kinds of assets. You may not be able to stop a competitor from using such assets, but you must always be sure that the attribution reflects your organization.

The complexity of network resources introduces difficult management and control questions. When we post content assets, we want our business associates to share them, but we must think about the security implications. For example, if I ask Mary to tell her network on Facebook about a great new video they should see, am I letting her go to Facebook to do whatever she wants there?

“ The complexity of network resources introduces difficult management and control questions. ”



## KEY LESSONS

- 1 THE TWO GREATEST SECURITY CHALLENGES WE FACE ARE THE SPEED AND VARIATION OF INNOVATIVE NEW ATTACKS AND THE COMPLEXITY OF OUR INFRASTRUCTURE.
- 2 WHEN WE POST CONTENT ASSETS, WE WANT OUR BUSINESS ASSOCIATES TO SHARE THEM, BUT WE MUST THINK ABOUT THE SECURITY IMPLICATIONS.

# GREATEST CHALLENGES: SPEED AND COMPLEXITY

It's not just Facebook, it's Facebook games, Facebook messaging, and all the other things she could access. If I allow her to go to Facebook, can she only go to the corporate page, or do I let her go to her personal Facebook page, too? This becomes a question about the application infrastructure. When you're talking about applications, it's not just whether you can or cannot use an app but also the functionality within the app. Which functions are permissible and which are not?

When addressing the speed issue, the constant barrage of innovative attacks, it is important to recognize that not all risks are equal. You must focus on the highest-risk problems first and in a way that does not create productivity problems. Recently, we added a next-generation firewall to our app security solution. It looks at patterns and behaviors to better understand the threats and performs real-time assessment of apps.

Addressing challenges of speed and complexity begins with a comprehensive security assessment that looks across your infrastructure, examines where your data are located and who shares them, considers compliance requirements, and evaluates your risk tolerance. Security policies must be granular and apply across all applications. Keeping up with continuously evolving security threats requires protection from real-time security services. The ultimate question in business is always one of money. Therefore, a business must define its tolerance for risk and align its security strategy with that tolerance.

“

*A business must define its tolerance for risk and align its security strategy with that tolerance.*

”



# TOO MANY SOLUTIONS, NOT ENOUGH ANSWERS



**PATRICK  
PETERSON**  
CEO and Founder,  
Agari

Patrick Peterson is Agari's visionary leader and a pioneer in securing the email ecosystem. He joined IronPort Systems in 2000 and defined its email security appliances. He invented IronPort's SenderBase, the industry's first reputation service. In 2008, after Cisco acquired IronPort, Patrick became one of 13 Cisco Fellows. In 2009, he spun out the email security technologies he had developed at IronPort/Cisco into his own company, Agari.

You're trying to secure the enterprise but the front door is wide open. You don't seem to know how to close that door let alone lock it. Organizations have hit a terrible cycle in which it seems every one has been either breached or compromised in some way. IT pros are so busy trying to figure out how many criminals are in the house and what was taken that they aren't able to put their full force into trying to stop this vicious cycle. What's sorely needed is for enterprises to establish and act on open standards for information sharing to thwart these attacks.

Eight out of 10 cybercriminals are successfully hacking into companies' databases by using email as the attack vector. That is the one door IT pros have not been able to lock and the reason we expend such tremendous effort and expense to detect and respond to breaches. With so much effort focused on only the detection, it distracts from solving the underlying problem.

One indictment of both the industry and practitioners is that short-term priorities tend to drive us. Criminals have evolved in their sophistication and we are now in an asymmetric war in which they can try a multitude of techniques. These criminals can be successful just one time in 10—or even just one time in 1,000—and disrupt our businesses. To be sure their success is limited, businesses have responded by deploying solutions. The challenge, of course, is that solutions check in but don't check out, resulting in organizations mired in unmanageable legacy solutions. The key to addressing this issue is to select solutions that have strong application programming interface (API) capabilities and to develop security staff who make decisions based on business needs rather than on their own comfort level in administering the current solution.

## KEY LESSONS

- 1** ORGANIZATIONS ARE SPENDING SO MUCH TIME RESPONDING TO IMMEDIATE THREATS AND BREACHES THAT THEY DON'T HAVE TIME TO SOLVE THE UNDERLYING PROBLEM.
- 2** HOLISTIC SECURITY SOLUTIONS REQUIRE INDUSTRY STANDARDS AND SECURITY VENDORS THAT REALIZE THAT THEIR PRODUCTS ARE ONE PART OF A LARGER SECURITY STRATEGY.

*“ You're trying to secure the enterprise, but the front door is wide open. ”*





# TOO MANY SOLUTIONS, NOT ENOUGH ANSWERS

Businesses now have multiple security solutions, encompassing email, web, application vulnerability management, and network scanning apps. For example, I was talking to the chief information security officer of a medium-sized bank that had 55 security vendor solutions and only 45 employees. He needed everyone in the company to be a guru in at least one solution and a select few had to provide 24x7 support in two. Each solution may do an adequate job, but no one can actually hire, retain and manage staff to keep up with such a multitude of growing solutions.

Innovation by both cyber criminals and the companies they attack has led to this multipronged security solution. To learn how the criminals have gotten in, you might need to analyze the malware on the PC, go to a threat intelligence system for information about that malware, go to another system for logs and events from the compromised server and then look at your email and web systems. And all of this is before you even get to the back-end systems that may have been affected.

People spend hours or days trying to pull together disparate information about one event from their systems. Of course, before they even finish that exercise, it is uncertain how cybercriminals have infiltrated their systems and what information they have stolen.

The industry is at long last looking at information sharing and the inefficiency that arises from its current absence. We're starting to see more open standards and vendors that realize they play a role in a whole strategy that is bigger than the sum of its parts. People must get on board with open standards for information sharing and industry solutions to close that open door. They need to thwart these data breaches before they incur hundreds of thousands or millions of dollars in forensics and analysis costs.

“

*One indictment of both the industry and practitioners is that short-term priorities tend to drive us.*

”



**DAN  
TWING**

President and COO,  
EMA

Dan Twing is responsible for developing and executing strategic market research, delivering value to IT organizations through consulting engagements, and directing product developments and marketing efforts. He leads the analyst team covering IT management topics such as systems, end points, storage, security, network and service management, and business intelligence and analytics. Dan joined EMA in 2005 and has more than 30 years of experience in information systems, software development, and technology outsourcing.

    
Twitter | Website | Blog

I have five key points for securing a network and application infrastructure. The first is staff and their skills. There's a shortage of the skill sets required in this line of work. Even if the resources are available, companies often can't deploy as many people as they need to get the job done properly. Security budgets have rebounded 10 percent to 14 percent over the past two years, but 68 percent of organizations still cannot find the staff to meet their needs. Those data points come from recent research that my organization did on what we call *data-driven security*.

The second point concerns legacy applications. Everybody wants to move faster, shift to containerized technology for applications, and use DevOps for continuous delivery. All that change and all those new applications get all of the resources, which means that there's not enough time for security to focus on the legacy apps because the new functionality is prioritized. As with personal self-defense, you have to have *situational awareness*—looking not just forward, but to the sides and behind you. In IT, you need to look backward toward your legacy applications and their unique security vulnerabilities while also looking toward the technology of the future as new threats develop.

The third point involves creating a unified access infrastructure for all environments. When everything was driven off a single identity store, like Active Directory or LDAP (Lightweight Directory Access Protocol), it was possible to centrally manage the environment. Now, however, you have geographically dispersed staff and people working from home.

“ There's a shortage of the skill sets required in this line of work. ”

## KEY LESSONS

- 1 IF YOUR ENVIRONMENT REQUIRES RAPID CHANGE, YOUR SECURITY PROCESSES MUST BE APPROPRIATELY RESOURCED TO MATCH THE PACE OF CHANGE.
- 2 PROPER ANALYTICS ARE ESSENTIAL FOR PREDICTING AND MANAGING SECURITY INCIDENTS REGARDLESS OF WHETHER YOUR SECURITY TEAM IS FULLY STAFFED.



Things have become more compartmentalized and distributed through public and hybrid cloud infrastructure, so it's become even more difficult to have a unified point of access.

The fourth point centers around the need for security analytics, including behavioral analytics, anomaly detection, and predictive analytics. Looking at log files, finding patterns, and being able to predict or see an attack as it's forming are key to solving many security problems. Being able to see an attack as it's building, to issue an alert and react to it before it gets out of control while navigating the alert storm and figuring out the root cause are important. Even if you have good tools that offset the lack of staff, you still can't manage security incidents without the proper analytics.

The fifth and final point is maintaining proper change control both on the infrastructure and on the applications. It's not just an operations issue but a security issue, too. When you make changes of any kind, you could be opening a security hole and introducing new vulnerabilities. Having a good change management process and good change management tools are important for keeping the network and the applications locked down, making sure everything is properly configured, and having good control over that environment. If you try to move to DevOps or to a continuous delivery environment in which you're going to increase the rate of change, you had better have a good change management process in place to handle the faster pace.

By addressing these five points, you can create a more secure network environment at your organization. Doing so requires a long-term investment of both human and financial resources, but it is well worth the effort.

“

*When you make changes of any kind, you could be opening a security hole and introducing new vulnerabilities.*

”

# MAKING THE BUSINESS CASE FOR STRONGER SECURITY



**DAVID  
HARLEY**

Senior Research Fellow,  
ESET

IT security researcher David Harley is an author and editor living in the United Kingdom, known for his books on and research into malware, Mac security, antimalware product testing, and email security. After 11 years with the Imperial Cancer Research Fund and moving into full-time security, he went on to run the National Health Service's Threat Assessment Centre. Since 2006, he has been a consultant to security company ESET, where he is a senior research fellow.

    
Twitter | Website | Blog

Working as an external consultant providing services to the security industry, I see many companies that can manage their own security perfectly well, and that has given me the opportunity to focus on specialist issues. Before I made that switch, though, I worked for a small medical research organization, and then for a huge and bureaucratic public health agency. In terms of protecting the network and infrastructure, these organizations presented very different challenges.

Regardless of the organization, however, it is important to recognize that no one spends money on security just because "everybody knows it's important." After all, what is obvious is not always true. For most companies, security is a cost center rather than a profit center, and its value is often too speculative to be instantly recognized, being based on events that might never happen. So, one of the greatest challenges in securing a company's infrastructure is persuading cost-conscious managers to spend as needed to build a level of security appropriate to their organization.

The construction of a security infrastructure appropriate to an organization's needs not only varies with the risks that that organization faces but also with resources available to it.

*“For most companies, security is a cost center rather than a profit center, and its value is often too speculative to be instantly recognized, being based on events that might never happen.”*

## KEY LESSONS

- 1 ONE OF THE GREATEST CHALLENGES IN SECURING A COMPANY'S INFRASTRUCTURE IS PERSUADING COST-CONSCIOUS MANAGERS TO SPEND AS NEEDED TO BUILD A LEVEL OF SECURITY APPROPRIATE TO THEIR ORGANIZATION.
- 2 SUCCESS IS LIKELIER WITH PLANNING BASED ON METICULOUS RISK ASSESSMENT, CLEAR ROLES AND RESPONSIBILITIES, AND REALISTIC TARGETS.



# MAKING THE BUSINESS CASE FOR STRONGER SECURITY

Not all organizations have the resources or the will to implement a full-blown security initiative based on standards such as PRINCE project management or ISO 27001, but smaller organizations can learn from these approaches. Don't base your security strategy on a limited range of prescribed offerings. Identify the security controls you need, and then research the most suitable implementations for your environment. Distrust panaceas. For example, specialist software may be better at catching advanced persistent threats (APTs) than end point antimalware solutions, but the latter catches a lot of low-level, untargeted threats that APT-specific solutions tend to miss. A Swiss Army knife is nice to have, but sometimes you need a full toolbox.

A wide range of persuaders might go into building a business case for stronger security. Sometimes, the driver is a high-profile security breach originating in inadequate controls. Back in the mid-1990s—this was pre-Mac OS X, at a time when replicative malware of all sorts was far more common—funding for Mac antivirus suddenly became magically available where I worked after I cleaned several hundred macro-viruses off the boss's laptop. However, being the company Cassandra isn't always a safe strategy. Sometimes, being right but unpersuasive is a punishable offence. Let me introduce you to [Professor Eugene Spafford's first principle of security administration](#): "If you have responsibility for security, but have no authority to set rules or punish violators, your own role in the organization is to take the blame when something big goes wrong."

Ideally, an organization will recognize the need to build a more secure infrastructure before a big security breach has occurred, not after. The consequences can range from being subject to legal action and penalties for non-compliance with mandated requirements to the loss or exposure of critical data, and can result in the total shutdown of an operation.

Skills required to assemble and present a business case for stronger security are often quite different to those necessary for hands-on implementation and administration of the security infrastructure. A major security initiative is usually better implemented as a team effort. Even a relatively small project, like transitioning a desktop security package, can have broad implications outside the expertise of a single tech security person. Success is likelier with planning based on meticulous risk assessment, clear roles and responsibilities, and realistic targets.

“

*A Swiss Army knife is nice to have, but sometimes you need a full toolbox.*

”

# DON'T FORGET THE BASICS



**RYAN  
DEWHURST**

Senior Research Fellow,  
Dewhurst Security

Ryan Dewhurst is a passionate information security professional who has more than six years of experience in the industry. He gained his first-class honors degree in computer security and has also received industry awards such as the *SC Magazine* Europe Rising Star award. Ryan is the founder of popular security-related projects such as DVWA and WPScan.

    
Twitter | Website | Blog

In doing some testing for a client recently, I was impressed at the level of software patches and updates the client had deployed. The organization was seemingly secure. I couldn't find many exploitable vulnerabilities that would give me a foothold in the company's network. Then, I came across a web login interface. While setting up a password dictionary attack against the service, I tried the most insecure login user name–password combination I know: *admin:password*. Lo and behold, I was authenticated. This was during setup: I hadn't launched the attack, yet!

This service stored all the client's customer proposals and receipts, all its billing information, and the names and passwords of the system's users. I suddenly had access to a treasure trove of sensitive corporate information.

Basic problems like this are the biggest challenges my clients face. Here are three essentials about which I am constantly reminding clients:

- **Use secure passwords.** Require your organization's user base to choose complex passwords that include numbers, upper- and lowercase letters, and special characters—no more *password* or *password1*, no more variations of your organization's name, no more names of pets. In addition, consider using long passwords, known as *pass-phrases*. You could encourage your users to use password managers, although these tools are not without their own issues.

“Require your organization's user base to choose complex passwords that include numbers, upper- and lowercase letters, and special characters—no more *password* or *password1*.”



## KEY LESSONS

- 1 THE GREATEST AND POTENTIALLY MOST DEVASTATING SECURITY CHALLENGES ARE THE MOST BASIC ONES.
- 2 SOFTWARE INFRASTRUCTURE IS CREATED BY HUMANS AND SO IT WILL ALWAYS BE VULNERABLE.



# DON'T FORGET THE BASICS

- **Keep software up-to-date.** I conduct internal penetration tests that still reveal the presence of the infamous MS08-067 vulnerability, which allows an attacker to execute arbitrary code on your servers. That vulnerability was discovered in 2008, and securing against it requires a simple patch. MS08-067. Such known vulnerabilities should be much more difficult to identify years after a patch has been made available, but in some cases, the patches aren't being applied, possibly because administrators aren't aware the patches are available or even that the vulnerability exists. Sometimes, administrators don't want to execute software updates out of fear that they might "break" something. Whatever the reason, it is up to individual organizations to manage their own risk and decide where it makes business sense to invest their resources. Keeping software updated is the most effective way to reduce risk while not taking up too many resources.
- **Test your software.** Regardless of whether an enterprise writes applications internally or purchases them from third-party providers, it must accept responsibility for ensuring that the software is written securely. For self-produced software, the chief information officer can impose that requirement in house by implementing a security development life cycle, but testing purchased software is also possible. Either have the provider hand over prior security testing documentation or hire a consultant to perform the testing for you.

No sufficiently complex system will ever be 100 percent secure. Software is written by humans, humans make mistakes, and mistakes manifest as bugs. Even with their extensive resources, Facebook and Google are not immune to software vulnerabilities. The best we can do is secure systems and bring the risk down to a manageable level.

Get the basics right, and you'll already be ahead of the pack.

“

*Such known vulnerabilities should be much more difficult to identify years after a patch has been made available, but in some cases, the patches aren't being applied.*

”



# Protecting the Core of Your Network

## In this Section...

---



**Alex Papadopoulos**  
Striata Inc.....23



**Dave Waterson**  
SentryBay.....29



**John Maddison**  
Fortinet, Inc.....25



**Linda Cureton**  
NASA.....31



**Robert Shullich**  
AmTrust Financial  
Services.....27

# MANAGING VENDOR SECURITY IS CRITICAL TO OUR BUSINESS



**ALEX  
PAPADOPULOS**  
Head of Operations,  
Striata Inc.

Alex Papadopoulos is the head of operations for Striata America and currently heads up all technical operations for North, Central, and South America. He is responsible for all areas of technical and project operations, including project management, support, development, and project implementation. Alex has more than 12 years of experience in the IT field, primarily focused on electronic billing presentment, billing, and supply chain management.

 |  |   
Twitter | Website | Blog

In providing electronic billing services to clients as well as sending and receiving emails associated with billing and payments, we deal with our clients' customer data. Ensuring the security of that data is an essential aspect of our businesses. Our two greatest security concerns are managing hosting vendors whose services we use and managing inadvertent or accidental breaches by staff.

As far as vendor management goes, this is important because we don't physically manage our own data and application servers. Instead, we rely on third-party hosting providers for our hardware and network infrastructure. Every business is a potential target, and the more data it processes, the bigger a target it is. We do not handle actual payments, so we don't have credit card data or information that would enable funds transfer, but there is always the possibility that somebody could use our data in a fraudulent billing scheme, so we must be vigilant. At the end of the day, however, the responsibility for any losses that affect our clients is ours.

To manage expectations and foster confidence in our ability to deliver on security promises, we perform a full security evaluation of our vendors, determining whether they follow best security practices, how they secure their data, and how they secure their facilities.

*“ Our two greatest security concerns are managing hosting vendors whose services we use and managing inadvertent or accidental breaches by staff. ”*

## KEY LESSONS

- 1** LOOK FOR VENDORS THAT ARE TOTALLY OPEN WITH YOU ABOUT EVERYTHING AND WHO ARE FLEXIBLE IN ADDRESSING ACTION ITEMS THAT NEED TO BE ADDRESSED.
- 2** ONE BIG CONCERN IS PEOPLE TAKING INADVERTENT OR ACCIDENTAL ACTIONS THAT INTRODUCE RISKS TO THE OPERATION.



# MANAGING VENDOR SECURITY IS CRITICAL TO OUR BUSINESS

We have detailed security policies that specify everything from how we manage our internal systems to security requirements and expectations of our vendors. We build these expectations into our SLAs, and we visit the physical locations of vendor data centers to see for ourselves how well the vendors protect their facilities. We often bring clients on these visits to demonstrate to them that the data they are entrusting to us are secure. We look for vendors that use an approach similar to ours. We define what we want and need from a vendor, and then perform annual reviews of the controls and policies.

Our other big concern is people taking inadvertent actions that introduce risks to the operation. We track every action taken. Then, red flags alert us if employees or customers take an action without understanding its potential consequences, such as clicking a phishing email or providing a credential that can then be used to gain unauthorized entry to a system or process.

Protecting against such accidental situations requires continuous education. For example, we send fake phishing emails to staff; anyone who clicks them is not reprimanded, but the episode becomes an opportunity to educate them on the risk and the proper way to handle suspicious communications. Continuous training and education are incredibly important.

To secure against human error, policies must be well defined, in place, and updated regularly. New staff must be trained on security policies before being given access to any systems. Staff must be regularly updated if a policy changes and re-trained at least annually. Finally, always test staff as a way to identify weaknesses, strengthen training, and improve policies.

“

*We have detailed security policies that specify everything from how we manage our internal systems to security requirements and expectations of our vendors.*

”

# SECURING VITAL DATA IS THE GREATEST CHALLENGE



**JOHN  
MADDISON**

Vice President, Marketing,  
Fortinet, Inc.

John Maddison has more than 20 years experience in the telecommunication, IT Infrastructure and security industries. Previously he held positions as General Manager Data Center division and Senior Vice President Core Technology at Trend Micro. Before that John was Senior Director of Product Management at Lucent Technologies. He has lived and worked in Europe, Asia and the United States. John graduated with a Bachelor of Telecommunications Engineering degree from Plymouth University, United Kingdom.



Website |



Blog

The greatest vulnerability for many businesses, especially mid-sized companies, is data vital to daily operations. We worked with a machine shop that used computer-controlled machines to create parts. Periodically, the shop would connect to the Internet to update its machines; somewhere along the way, the company picked up malware that remained dormant in its system. After a time, when the shop went onto the Internet again, the malware received an instruction and immediately encrypted all the data the shop's very expensive machinery needed to operate. Soon after, the company received a ransom email asking for \$50,000 in exchange for decrypting the data. The business had little choice. A week with idle machines would have bankrupted it, so it paid the ransom, the data was decrypted, and it was up and running again.

Most businesses today depend on data, whether it is unique intellectual property or simply data that enable them to operate. Losing that data would literally put them out of business. So, how do you protect that vital asset? You must protect the network, which also includes people who use the network and all the devices connected to it. This is becoming an increasingly difficult task.

As businesses build infrastructures, they are extending beyond their core systems to data centers, cloud services, and mobile devices; managing connectivity to the Internet; and making sure their core network provides all the services their users need. Performance is a key factor.

*“ Most businesses today depend on data, whether it is unique intellectual property or simply data that enable them to operate. ”*

## KEY LESSONS

- 1** THE REAL PROBLEM FOR SMALL AND LARGE BUSINESSES ALIKE IS NOT HAVING THE RESOURCES THEY NEED TO IMPLEMENT SECURITY THEY SHOULD HAVE FOR THE LEVEL OF PROTECTION THEY REQUIRE.
- 2** YOU MUST PROTECT THE NETWORK, WHICH ALSO INCLUDES PEOPLE WHO USE THE NETWORK AND ALL THE DEVICES CONNECTED TO IT.



# SECURING VITAL DATA IS THE GREATEST CHALLENGE

Users expect high performance from their dispersed network infrastructure. With all this going on, the network boundary becomes larger and more porous, which makes it more vulnerable.

One approach is for companies to think about their infrastructure as being made up of an internal network and an external network. They can apply their own security solutions to their internal network. Securing the external network involves applying policies and procedures and relying on SLAs with service providers, but there are limits to what they can do with that, which means that a certain level of risk will always be associated with their external network. It comes down to levels of trust in different parts of the network.

One strategy we are seeing is companies securing their internal network from within. They do this by segmenting their core network, breaking it down based on users or applications or traffic or other criteria. Then, they apply trust levels to each segment. They can implement different levels of protection between different segments based on the trust level between those two segments. Anything passing from one segment to another must pass that segment's trust-level security protections. In this way, if a threat breaches one segment, the chances of it spreading across the internal network are much less.

The real problem for small and large businesses alike is not having the resources they need to implement security they should have for the level of protection they require. They often do not discover this until after they have experienced a breach. Finding the right balance among cost, levels of security, and data protection is not easy. Businesses need a trusted partner that has qualified and certified staff. The business should build a personal relationship with that trusted partner.

“

*One strategy we are seeing is companies securing their internal network from within.*

”



# THE DISAPPEARANCE OF THE PERIMETER IS THE GREATEST SECURITY CHALLENGE



**ROBERT  
SHULLICH**

Enterprise Security  
Architect,  
AmTrust Financial Services

Robert Shullich is an enterprise security architect at AmTrust Financial Services. He has worked in the financial services sector for more than 30 years, having held senior-level roles in information risk and information security. In his current role, he assesses information risk for IT projects and proposes additional controls or design changes that will reduce the risk to the project. He has also taught cyber-risk management at the graduate level.

   
Twitter | Website

Enterprise computing today is made up of a mixture of in-house systems; cloud-based services; a diverse collection of mobile devices that employees use to access data from anywhere; and even consumer-grade cloud-based services, such as file sharing, that the enterprise may not know its employees are using. It is difficult in this environment to have an accurate idea of what your assets are and who is using or should be allowed to use them. Many organizations lack inventories of assets, including employees, software, hardware, and data centers. The reality is, you can't protect what you don't know you have.

This lack of complete situational awareness is a result of the evaporation of the legacy concept of the *perimeter*. We have punched holes in that perimeter to allow employees access to internal networks for work-at-home scenarios, to provide mobile salespeople the ability to more effectively service new and current customers while traveling, and to outsource operations of our networks to third parties. The data all these people access with their smartphones and tablets must be protected, but in this environment, it is often difficult to know where that data is.

Consider, for example, a typical third-party cloud service provider that is delivering a Software as a Service business application that depends on your critical business data. As part of your SLA, you may require the third-party vendor to ensure certain levels of risk abatement and threat protection.

“ It is difficult in this environment to have an accurate idea of what your assets are and who is using or should be allowed to use them. ”

## KEY LESSONS

- 1 MANY ORGANIZATIONS LACK INVENTORIES OF ASSETS. THE REALITY IS, YOU CAN'T PROTECT WHAT YOU DON'T KNOW YOU HAVE.
- 2 THIS LACK OF COMPLETE SITUATIONAL AWARENESS IS A RESULT OF THE EVAPORATION OF THE LEGACY CONCEPT OF THE PERIMETER.





# THE DISAPPEARANCE OF THE PERIMETER IS THE GREATEST SECURITY CHALLENGE

However, it is likely that the vendor is relying on a fourth-party cloud service provider to store your data. So, where is your data *really*, and how do you assess the risks to your data if it is difficult to know exactly where it is physically located.

Another problematic area for some companies is employees' use of low-cost file-sharing services without the knowledge of security people. This is typically not a malicious act: it is simply a case of employees trying to do their jobs as efficiently as possible. Nevertheless, it exposes proprietary data to risk, and if the practice is unknown to those who manage corporate security, it represents a risk they cannot see or defend against.

To address these security challenges, organizations need to start with accurate asset inventories. Whether an asset is purchased, leased, or acquired as a service, it must be tracked for its entire life cycle. An entire life cycle begins with acquisition or creation, carries through maintenance, and ends with destruction. Assets include hardware, software, data, and even people. Assets should be classified so that the organization knows what they are and how much protection each asset requires. Organizations need to integrate all business processes with asset acquisition so that expenses and purchases can be tracked. Loopholes in expense tracking allow employees to purchase cloud instances on a credit card and build applications that bypass IT governance processes. Above all, organizations need clear written policies and procedures on the handling of assets and an effective communications and training program (security awareness) to reinforce adherence to those policies.

The reality here is that most businesses are not in the business of fighting malicious hackers. They are in the business of doing their business. They have a security department or person who does the best job possible to address the highest-risk issues so the business can minimize risk to its revenue-generating operations. But they are up against professional data thieves who operate 24x7 to figure out how to steal that data. The security person needs to get it right every hour of every day; the data thieves need to get it right only once.

“

*The security person needs to get it right every hour of every day; the data thieves need to get it right only once.*

”





**DAVE  
WATERSON**  
CEO,  
SentryBay

Founder and chief executive of SentryBay Limited, Dave Waterson is an information security technologist and inventor of patented technology in the anti-key logging and anti-phishing areas. Based in London, United Kingdom, Dave has guided the company from startup to become a recognized leader in its sector of information security software development, with security solutions for PC, mobile, the cloud, and the Internet of Things. He has a master's degree in economics and is a registered CISSP.

Organizations used to focus security on the enterprise network perimeter. Organizations built virtual walls—firewalls and demilitarized zones—at the periphery to stop people from getting inside. Unfortunately, the network was breached anyway.

Then, the industry shifted focus to endpoints - PC equipment and mobile devices. Antivirus applications became our shields of choice. Sadly, we now know that antivirus software grows less effective daily.

My view is that we need to shift the defenses closer to the enterprise core—down to the granular level of data, where several big challenges await:

- **Personal information.** Personally identifiable information (PII) is an enormous enterprise problem—the Sony Pictures Entertainment and Target Store hacks demonstrate just how enormous. Many enterprises hold the PII data of millions of people within their IT core.
- **Cloud computing.** There are actually two challenges here. First, the cloud technically extends the enterprise network beyond direct enterprise control. Second is the sheer volume of data. Cloud computing offers far greater storage and process volume than companies have ever had. Security issues arise from both.

“ I recently wrote a blog post in which a fictitious IoT-enabled garage door becomes part of an attack botnet. ”

## KEY LESSONS

- 1 THE FOCUS OF ENTERPRISE NETWORK SECURITY NEEDS TO SHIFT CLOSER TO THE ENTERPRISE CORE—TO DATA.
- 2 BEYOND TECHNICAL SOLUTIONS, PROCEDURES AND RAPID RESPONSE TEAMS NEED TO BE PUT IN PLACE.



# CLOSER TO THE HEART

- **The Internet of Things (IoT).** The IoT is not a big factor yet, but every company is examining it. In factories and retail, data-producing sensors will be attached to almost everything. The IoT will control office energy settings and meeting room management. Attack surfaces will multiply exponentially. I recently wrote a blog post in which a fictitious IoT-enabled garage door becomes part of an attack botnet. That might give you some idea of the scale of this impending danger.

So, how do we meet these challenges?

First, we keep protecting the perimeter. Web application firewalls, intrusion-detection and prevention services, honeypots, and all the rest remain crucial. These are the sentries at the gate that can radio into headquarters when something is amiss.

Next, figure out what data you have. A surprisingly large number of enterprises do not know this. After that, track data flows throughout the organization. Where and how are data coming in? Where do they sit around unencrypted? What are the attack vectors at each phase of data flow?

Finally, carefully assess what types of data need to be secured. Some data, frankly, needs little security—they just are not that sensitive. Knowing which data types are where will allow you to target security investment where it has the greatest payoff.

If it sounds as if a big data solution is where this is heading, you are right. Big data technologies (Apache Hadoop, in-memory computing [IMC], Scala, Spark, etc.) offer the measurements, machine learning, and early warnings that can show you if and where security breaches exist. Securing data at entry is also important. Beyond the purely technical solutions, you need to establish procedures and assemble a well-trained, rehearsed, and practiced response team that can spring into action immediately.

I think companies today realize that it is not a matter of *whether* they will get breached but *when*. The secret in securing the enterprise network is to focus at the level of data.

“

*I think companies today realize that it is not a matter of whether they will get breached but when.*

”



**LINDA  
CURETON**  
Former CIO,  
NASA

Linda Cureton is CEO of Muse Technologies and former CIO of NASA, with more than 34 years of service in IT management and at the U.S. federal cabinet level. She holds a B.S. degree in mathematics from Howard University and an M.S. degree and a post-master's advanced certificate in applied mathematics from Johns Hopkins University. A strategic innovator, thought leader, prolific blogger, and pathfinder for federal CIOs using social media, Linda has received many awards and is a bestselling author.

    
Twitter | Website | Blog

Protecting data and understanding the risks data faces are two of our greatest weaknesses. We have focused on protecting the perimeter and put so many resources into doing so that we have, perhaps, neglected the data itself, especially when you look at insider and advanced persistence threats. Protecting the perimeter doesn't necessarily afford you the protection you need: I think that our strategy needs to focus on protecting data.

This is not to say that you shouldn't protect the network, but I don't think that our defense matches our risks very well. One way to protect against insider threats is two-factor authentication (2FA), which uses what you know and what you have. The issue preventing adoption of 2FA might be the cost associated with it and the fact that legacy applications aren't always able to use such methods.

Another way is the protected data approach—basically taking the stance of “trusting no one.” Trust is verified: if you are who you say you are, prove it. When this approach has been applied and users have been verified, they can go anywhere and access anything on the network.

One example of how inside threats can compromise an organization is the breach that happened at the Office of Public Information several years ago. A person who was not authorized to access certain documents not only did but managed to take many off premises. In that example, we relied too much on passwords to secure things. We often think the solution is to change or strengthen passwords, but this issue is much larger than a password problem. Organizations need to understand that these threats go much deeper.

*“ I don't think that our defense matches our risks very well. ”*



## KEY LESSONS

- 1** UNDERSTAND THE THREATS THAT ARE SPECIFIC TO YOUR ORGANIZATION, AND DON'T FORGET TO LOOK AT THE THREATS THAT MAY COME FROM WITHIN.
- 2** DESIGN YOUR SECURITY PROGRAM BASED ON THE UNIQUE NEEDS OF YOUR ORGANIZATION RATHER THAN TRYING TO FIND A ONE-SIZE-FITS-ALL SOLUTION.

# TRUE SECURITY REQUIRES UNDERSTANDING AND A LAYERED SECURITY APPROACH

Understanding the threat and the risk factors help guide you to better defense approaches. A good way to better understand those risks is for organizations to think about them from the beginning. We spend a lot of time and resources on checking the box next to risk analysis, but we don't really dig in to figure out what the true risks are. We need to do a good, old-fashioned "What are our risks?" assessment. Those risks vary from organization to organization.

We also spend a lot of time and resources understanding compliance, and doing so can get in the way of finding the right kind of protection. We are pressured to comply with a laundry list of things that may or may not apply to our situation or organization. It would be better if we spent that time on risk assessment. If we understood our risks, we could then prioritize the laundry list, pick the most critical risks, and find the right solutions to mitigate them.

As it is, we have a tendency to look for a single solution that fits everyone, but the scenario just doesn't apply. There are a lot of security solutions out there, so many that it's becoming a problem. How do you choose the right solution? Some think all you have to do is have a firewall, but really, you've got to have a firewall, intrusion protection, good authentication mechanisms, good network topology—the list goes on—so that when a breach occurs you're able to recover better.

There is no magic bullet that addresses every security risk. True security requires a layered defense of several solutions, put together to give you the right kind of protection for your specific organization. No single tool will keep your network and data safe.

“

*True security requires a layered defense of several solutions, put together to give you the right kind of protection for your specific organization.*

”

# In cybersecurity, there's the slick SALES PITCH...

...and then there are facts.

**Our focus on innovation** over the last 15 years means you can simplify your security strategy and stay ahead of the threat today—not in an upcoming version that only exists in a pitch over golf.

We deliver a consolidated approach from datacenter to endpoint, plus global visibility and control on one OS with one management console.

**It's because we like our labs more than the golf course.**

Get a Cyber Threat Assessment today and get the facts about your security posture.

[www.fortinet.com/ctap](http://www.fortinet.com/ctap)

**FORTINET**®

**99%** effective breach detection

**5X NGFW** performance

**#1 unit share** worldwide in network security

**Over 200** zero-day attacks discovered



Data Center Firewall  
Next Generation Firewall  
Breach Detection  
Web Application Firewall

Security Without Compromise

# Staying Ahead of Hackers

In this Section...

---



**Tom Eston**  
Veracode.....34



**Will Lefevers**  
Constant Contact.....38



**Steven Weiskircher**  
ThinkGeek, Inc.....36





**TOM  
ESTON**

Manager, Penetration  
Testing,  
Veracode

Tom Eston is the manager of Penetration Testing at Veracode. His work over the years has focused on security research, leading projects in the security community, improving testing methodologies, and team management. He is also a security blogger; co-host of the Shared Security Podcast; and a frequent speaker at security user groups and international conferences, including Black Hat, DEFCON, DerbyCon, Notacon, SANS, InfoSec World, OWASP AppSec, and ShmooCon.

 |  | 

Once I was part of a no-holds-barred red team assessment of a famous actor. He had put a lot of digital safeguards in place and was confident his digital life was hack-proof. It wasn't.

As a first step, I had one of my team members place a phone call to Amazon tech support. He told the worker that he wanted to add a credit card to the actor's Amazon account. The staffer asked a security question: What is one of your most recent purchases? My staff member knew that our guy was a *Game of Thrones* nut, so our caller winged it. "*Game of Thrones*, DVD Box, Season 1," he said. "Right," the support worker replied. "We'll reset your password."

That single move gave my team access to a lot of the actor's personal details. It allowed us to hack into his Twitter account, then his email. We reset passwords to practically every account he had. Within days, we had infiltrated his entire digital life. Needless to say, the actor was shocked.

There is a lesson here for organizations: many respond to their vulnerabilities only after a breach. That's not good enough. My take is that the defensive corporate mindset needs to become proactive.

Here are three of the biggest electronic security challenges I see for companies that operate in the digital realm:

- **Social engineering.** Most corporate breaches start with phishing emails or phone calls or with an attacker physically walking into a building and claiming to work there. It's called *social engineering* because attackers take advantage of the natural human desire to trust.

“ That single move gave my team access to a lot of the actor's personal details. ”

## KEY LESSONS

- 1 MOST CORPORATE BREACHES START WITH SOCIAL ENGINEERING TACTICS.
- 2 APPLICATIONS VULNERABILITIES AND SYSTEM MISCONFIGURATIONS ARE TOO OFTEN OVERLOOKED.



# BECOMING PROACTIVE

From a computer security perspective, this is a dangerous attack vector—the same one my team used to hack our actor friend. It shocks me how easy the human factor is to exploit.

- **Application vulnerability.** Web applications are the front end of most organizations and the way most of them make money. In recent years, immense new layers of complexity have been introduced behind the scenes to allow apps to work in the cloud. With complexity comes human error. I often find that companies don't take the time to build security into their application infrastructure or to perform proper security testing from the beginning. This remains true even today, when security is top of mind with most executives.
- **System misconfigurations.** These, too, are often overlooked. Web management consoles, even production systems, often remain in their default configurations, accessible through default passwords. When hardening application coding and infrastructure that applications live on, spend some time focused on this piece. As an attacker, if I can access your web management console by using a default password, I no longer care about the application. I can access everything on your server.

The moral is simple: be vigilant. Continually educate your employees. Have third-party consultants conduct penetration tests, and be prepared to hear things you wish you hadn't—like you've already been hacked. Stage your own social engineering tests so that employees know what these attacks look like and what to do when they happen.

A lot of what we call *network security* is really just a question of human awareness.

“

*Stage your own social engineering tests so that employees know what these attacks look like and what to do when they happen.*

”



# WHAT KEEPS ME UP AT NIGHT



**STEVEN  
WEISKIRCHER**

Chief Information Officer,  
ThinkGeek, Inc.

Steve Weiskircher has more than 19 years of direct leadership experience in the e-commerce industry, having served as the chief information officer of multiple top “e-tailers,” including Crutchfield, Fanatics, and most recently ThinkGeek, where he is responsible for the technology and user experience teams. Steve holds a B.S. degree in mechanical engineering from Virginia Tech and an M.S. degree in management information systems from the University of Virginia.

   
Twitter | Website

Once, I tried to sell an executive management team on investing in an intrusion-prevention system (IPS) and web application firewall (WAF). They were not impressed. Who would attack us, they asked?

To answer that question, I set up a dummy server—with up-to-date patches—just outside the corporate firewall. Within three minutes, it was being robotically mapped and scanned. Within 12 minutes, it was under direct assault. That convinced them.

That was long ago, but people still see security investment as an insurance policy they will never collect on. That’s partly why these three challenges keep me up at night:

- **External predators.** These are the attackers and nefarious bots that beat on the door, day and night, pounding away at my perimeter defenses trying to break in. As an e-commerce retailer, we deal with these a lot. I also see the tertiary effects of other breaches—somebody’s account or credit card is compromised during another retailer’s breach. The nefarious individuals then use that account data on another site. More recently, I have seen a shift in this fraud where account data that was compromised during one of the mass breaches is sold or traded to another individual. That person attempts to buy product and return it for cash. They do not even have to go through the effort of hacking someone’s account, as there is ample supply of previously compromised accounts in the wild.

“ Within three minutes, it was being robotically mapped and scanned. Within 12 minutes, it was under direct assault. ”

## KEY LESSONS

- 1 EXTERNAL PREDATORS, INTERNAL THREATS, AND CRUMBLING NETWORK BOUNDARIES ARE BIG WORRIES.
- 2 THOROUGH RISK ANALYSIS SHOULD BE PART OF ANY NEW TECHNOLOGY IMPLEMENTATION, PARTICULARLY WHEN YOU WORK WITH EXTERNAL PARTIES.



# WHAT KEEPS ME UP AT NIGHT

- **Crumbling boundaries.** Familiar network and application boundaries are falling at an incredible rate. Cloud services, coupled with a next-generation Bring Your Own Device workforce, are blowing away the borders. We used to have nice, hardened perimeters, and extensive device management. That era has ended. We now have to protect our data in an always on, always connected world where there are no longer clear perimeter boundaries. Quite simply, we don't have the same measure of control anymore.
- **Internal threats.** These threats can come from disgruntled employees or contractors looking to profit off of your critical data. It is difficult to protect against every possible threat vector involving an internal employee that has access to sensitive data and the Internet. It has become too easy to shift large volumes of data relatively undetected. While this does occur, the more probable scenario is the unintentional hole that an employee or contractor creates. Outsourced third-party contractors can be a particular risk; they often have direct and/or privileged access into the interior of your network. The challenge is you do not manage their devices or the networks they connect into. Such unintentional exposures can create holes through all your defenses.

“  
*Security will always be a combination of advanced technology and smart people.*  
”

There are mitigation steps you can take, of course. Providers like Fortinet and others offer advanced IPS, WAF, and centralized login tools. These technologies are requirements for any public-facing web servers or exposed application programming interfaces. Regular threat assessments are also key. Internal and external vulnerability scans should be regular events. The days of simply instituting IP restrictions or even stateful firewalls are over.

For cloud-based risks, in conjunction with the threat-assessment piece, I recommend thorough risk analysis. That should also be part of any new technology implementation, particularly when you work with external parties. A full-on penetration test or vulnerability assessment starts with automated scanning, but you should also have your people performing careful risk-management assessments. What data does that server hold? What networks or systems can access it? Should you restrict access, or cordon it off all together?

It would be great if there were such a thing as a straight, universal security checklist. Unfortunately information security is not a recipe that we can follow. We live in a world of gray, not black and white. Therefore, security will always be a combination of advanced technology and smart people. It is only by carefully sorting through the risk factors that you can come up with the right strategies to mitigate the danger.

# HUNTING THE HUNTERS



**WILL  
LEFEVERS**

**Lead Information Security  
Architect,  
Constant Contact**

Will Lefevers is an information security architect who has 15 years of experience, including military tours in satellite operations, counterintelligence, cyber operations, and vulnerability research. Prior to joining Constant Contact, he was the application security engineer for a multimillion-dollar next-generation cloud platform. His foci include insider threat detection, behavioral analysis, malware reverse-engineering, and hunting threat actors in live networks. He's also an avid homebrewer and writes exceptionally mediocre code.



My greatest challenge is finding talent. The market is awash with people who claim they can do InfoSec. Bolstered by a master's degree in IT management, a freshly minted Certified Information Systems Security Professional certification, or a few years of managing firewalls, plenty of folks are willing to sign up to try network security. Most of them fall far short of the mark. I need hunters.

The industry sells all manner of fascinating tools to find the bad guys on your network. Intrusion-prevention systems, next-generation firewalls, big data security analytics—they all offer you the grail. They're each going to save you. Each claims to have built something that knows your network well enough to pinpoint aberrant behaviors in the vast oceans of noise. They all purport to find the needle in the haystack. I have yet to find one that does.

To be clear, I'm hunting hunters—people who think like the bad guys. People who study offense and keep up to speed on the latest developments in hacker subculture. People who can write exploits and malware and know exactly why that new vulnerability is going to spread like wildfire in the Russian underground. People who can quote off the top of their head the black market price of someone's full medical file. People who blend in with both the suits and the punks. People who make it their lifestyle to stay on the cutting edge of security. People who live it instead of just working it.

*“ My greatest challenge is finding talent . . . I need hunters. ”*

## KEY LESSONS

- 1** NOTHING BUT EXPERIENCE CAN TEACH YOU HOW TO RESPOND IN THE MOMENT WHEN YOU HAVE BEEN BREACHED. YOU NEED PEOPLE WHO WILL RUN TOWARD THE FIRE.
- 2** FINDING TALENTED PEOPLE WHO STUDY OFFENSE AND KEEP UP TO SPEED ON THE LATEST DEVELOPMENTS IN HACKER SUBCULTURE IS KEY.



# HUNTING THE HUNTERS

The reality is that each of us will be breached. We'll all get to experience that dazzling rush of panic and excitement. We'll all live under the pressure of unsteady upper management, certain that intense scrutiny will meet our every decision for the next few weeks. Maximum pressure will be applied with near-zero tolerance for common mistakes. Nothing but experience can teach you how to respond in that moment. In situations like that, I've seen two kinds of personalities: those who run from the fire and those who run toward it. I revel in those moments. I need people who run toward the fire. I need people who look forward to the next chance to prove their skills.

The hacker world evolves in response to every new defense. The cat-and-mouse game between attacker and defender plays out continuously. At the end of the day, shiny toys and fancy degrees won't save you. I need the hackers who hunt hackers.

“

*The reality is that each of us will be breached. We'll all get to experience that dazzling rush of panic and excitement.*

”



# Protecting Against APTs and Application-based Attacks

In this Section...

---



**Mikhael Felker**  
VC backed eCommerce.....41



**Erlend Oftedal**  
F-Secure.....43

# APPLICATIONS REPRESENT TODAY'S GREATEST SECURITY RISKS



**MIKHAEL  
FELKER**

Director of Information  
Security,  
VC backed eCommerce

Mikhael Felker is the director of information security at a growing venture in Santa Monica, California. His professional experience is a confluence of information security, privacy, teaching, technical journalism, and nonprofit leadership in such industries as defense, health care, nonprofit/education, and technology. Mikhael received his M.S. degree in information security policy and management from Carnegie Mellon University and B.S. degree in computer science from UCLA.



In a modern network and application infrastructure, the application has become the greatest point of risk for several reasons. One is that there is a proliferation of apps, made possible because apps are easier to build than ever. The number of apps appearing in a typical business environment is increasing, and these apps are evolving rapidly. Unfortunately, the resources available to address any security issues these apps may create is comparatively fixed. Several business dynamics aggravate the problem of application security.

There was a time when the infrastructure was on premises and development cycles were not as fast as they are today. In such an environment, securing the infrastructure was easier. Now, with complex hybrid environments and demand for rapid app development cycles, it is much more challenging to build secure apps in the time in which they are needed. Each business unit might have its own environment and work with its own vendors, and these environments are constantly changing. IT staff create and tear down virtual private networks.

With a real-time picture of the environment, organizations can focus on the highest security priorities, but gaining that total view of the environment is difficult. Products are available that help aggregate a view of the business environment. Analytics and visualization tools can give IT staff a snapshot of the environment, which they can then use to prioritize security efforts.

“ Fixing known flaws . . . comes down to prioritizing development efforts for revenue-generating app features over maintenance. ”

## KEY LESSONS

- 1 THE NUMBER OF APPS APPEARING IN A TYPICAL BUSINESS ENVIRONMENT IS INCREASING, WHILE THE RESOURCES AVAILABLE TO ADDRESS SECURITY ISSUES THOSE APPS MAY CREATE IS COMPARATIVELY FIXED.
- 2 EVEN IF YOU CAN NARROW A LIST OF KNOWN FLAWS TO THE HIGHEST-RISK ITEM, YOU STILL MUST PRIORITIZE THAT FIX AGAINST THE REVENUE POTENTIAL OF BUILDING NEW FEATURES.



# APPLICATIONS REPRESENT TODAY'S GREATEST SECURITY RISKS

Even with snapshots of a complex, ever-changing environment, though, other challenges to building secure apps exist related to prioritizing development efforts and the allocation of development resources. Regarding prioritization, let's assume that the IT organization knows every vulnerability in an app and fully understands the business use cases subject to abuse. The IT organization must prioritize fixing those flaws over building new functions, so it comes down to prioritizing development efforts for revenue-generating app features over maintenance. Even if IT can narrow a list of known flaws to one high-risk item to fix, they must still prioritize making that fix against the revenue potential of building new features.

Compounding the prioritization problem is resource allocation. When looking at overall app security, the organization must look at the broad spectrum of app services, mobile apps, and application programming interfaces. It must also consider the app environment—on premises, Platform as a Service, or Infrastructure as a Service. There is such pressure to build and launch apps quickly that organizations often lack the resources to test the app in all the environments in which staff may use it.

This combination of a growing number of apps, allocating resources to build and test for increasingly complex hybrid environments, and prioritizing security fixes against developing new revenue-generating features is a recipe that makes apps perhaps the greatest security risk businesses face today. With this security challenge in mind, it is more important than ever to involve information security professionals at the earliest stages of business projects, including security and compliance requirements, and to minimize risk and project rework. It is also important to leverage existing standards, frameworks, and methodologies such as the National Institute of Standards and Technology and the International Organization for Standardization to ensure that projects have a security baseline.

“

*It is more important than ever to involve information security professionals at the earliest stages of business projects.*

”



## ERLEND OFTEDAL

Senior Security Consultant,  
F-Secure

Erlend Oftedal has worked as a software developer and security tester for more than 10 years. He has spoken at several security and developer conferences and also develops open source security tools. Erlend is the head of the Norwegian OWASP chapter.



It is important to recognize that no matter how many protections we build into our infrastructure, we will always have vulnerable systems. The real security threat comes from not detecting attacks soon enough and not responding to them quickly enough. Many of the highest-profile security breaches in recent years went on for many months before they were detected.

So, what contributes to insecure networks and infrastructure?

A big factor is the growing complexity of networks and software environments. Businesses often have a variety of systems they have acquired over the years, including applications built on old frameworks and libraries that no one in the company knows anything about any more. Sometimes, the original manufacturer of an application is no longer in business, and the company would rather develop new code than fix old vulnerabilities.

Software itself is becoming more complex and more dependent on third-party code. Ten years ago, according to studies, 80 percent of code in a new application was custom built and 20 percent came from libraries. Today, 20 percent of new applications are made with custom code, and 80 percent of the code comes from libraries. Application development has changed to include more security testing during the development process, with tools that detect vulnerable library code and security routines built in at the unit testing stage. Still, developers make mistakes. Users make mistakes, too.

*“ No matter how many protections we build into our infrastructure, we will always have vulnerable systems. ”*

### KEY LESSONS

- 1 AS LONG AS VULNERABLE LEGACY APPLICATIONS EXIST, DEVELOPERS MAKE MISTAKES, AND USERS DO THINGS THEY SHOULDN'T, ATTACKERS WILL GET INTO THE SYSTEM.
- 2 NEW TOOLS ENABLE DEVELOPERS TO BUILD ACTIVE SECURITY MONITORING INTO THE APPLICATIONS THEMSELVES.



# DELAYED THREAT DETECTION AND SLOW RESPONSE POSE THE GREATEST THREATS

As long as vulnerable legacy applications exist, developers make mistakes, and users do things they shouldn't, attackers will get into the system. The best protection against these threats is early detection and rapid response. Companies rely on solutions such as next-generation firewalls and honeypots to protect against known threats and look for suspicious activity that may indicate a previously unknown threat. A new approach to software development that may be even more effective for some kinds of applications involves new tools that enable developers to build active security monitoring and sensors into the applications themselves. If the application detects any violation of its known operational behavior, it can send alerts, block an activity, or stop the application altogether. Every application would be built with security checks specifically designed to protect that application against illegal behaviors. The advantage over generic security solutions is that generic solutions never know exactly how an authorized application is supposed to behave.

As our lives become more dependent on software at work, in our homes, and even in our cars, it is essential that we have visibility that allows rapid detection, quick response to contain attacks of all kinds and fast deployment of mitigations when vulnerabilities are uncovered.

“

*The best protection against these threats is early detection and rapid response.*

”

# In cybersecurity, there's **A LOT OF HYPE...**

**...and then there are facts.**

**Flashy marketing** has a way of clouding the truth: slow is broken. You don't have to choose between having a strong security posture and having optimal network performance to power your business.

**You can have both – but only from us.**

Get a Cyber Threat Assessment today and get the facts about your security posture.

[www.fortinet.com/ctap](http://www.fortinet.com/ctap)

**FORTINET®**

**99%** effective breach detection

**5X NGFW** performance

**#1 unit share** worldwide in network security

**Over 200** zero-day attacks discovered



Data Center Firewall  
Next Generation Firewall  
Breach Detection  
Web Application Firewall

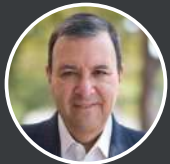
Security Without Compromise



# The Human Factor and a Culture of Security

In this Section...

---



**Michael Krigsman**  
cxotalk.com.....46



**Matthew Witten**  
Martin's Point Health Care.....53



**David Fosdike**  
IT Investigations.....48



**Peter Schawacker**  
Optiv Security, Inc.....55



**Simone Jo Moore**  
SJM.....50



**Scott Stewart**  
Deloitte.....58

# SECURITY IS A TECHNICAL AND A HUMAN PROBLEM



**MICHAEL  
KRIGSMAN**

Industry Analyst and  
Founder,  
cxotalk.com

The founder of cxotalk.com, Michael Krigsmann is recognized internationally as an industry analyst, strategy advisor, enterprise advocate, and industry commentator. As a columnist for ZDNet, Michael has written more than 1,000 articles on enterprise software, the cloud, CRM, ERP, collaboration, and alignment between IT and lines of business. Michael is often a judge for such prestigious industry contests as the CIO100 (*CIO Magazine*) and CRM Idol. He is also a photographer whose work has been published by *The Wall Street Journal*, MIT, and CNET News.

    
Twitter | Website | Blog

Organizations today are challenged by security risks at both the technical level and the human level. At the technical level, network security has become extremely complex because networks have become more complex. To be effective, business operations have come to depend on advanced network architecture and infrastructure. Maintaining and securing this kind of infrastructure, architecture, and capability is out of reach for most small to mid-sized businesses and challenges even the largest enterprises.

On the human side, governance, processes, skills, and judgment must come together to ensure that the best decisions are made and operations remain secure. It is not just outside threats that are a problem. Organizations must remain vigilant against unauthorized internal activities, either malicious or simply accidental. Judgment and decision-making are critical components in maintaining security.

The human and technical aspects typically work together to compound the security challenge. For example, many companies prefer to use on-premises applications and systems rather than cloud-based solutions because they feel more comfortable controlling their own security than outsourcing it to the cloud provider. This perspective is understandable, but the reality is that few organizations, regardless of their size, can match the security and skills that cloud services providers can offer. Although perceptions are changing around cloud security, many IT leaders cling to the notion that their in-house security is better than what a large cloud provider can offer—this despite the greater investment and specialized skills that cloud providers bring to the problem.

## KEY LESSONS

- 1 THE HUMAN AND THE TECHNICAL TYPICALLY WORK TOGETHER TO COMPOUND SECURITY CHALLENGES.
- 2 NO ONE KNOWS WHERE THE NEXT BIG THREAT WILL COME FROM.

“ Network security has become extremely complex because networks have become more complex. ”



# SECURITY IS A TECHNICAL AND A HUMAN PROBLEM

Another area where human and technical considerations come into play relates to mobility. Mobile technologies are a special challenge, because through them, businesses are potentially bringing internal data to the periphery of the network and beyond to a geographically dispersed group. The data no longer reside in the physical confines of the company's building or defined network infrastructure. Users want complete access to data on their mobile devices, which means that any one of those devices can become an entryway into the corporate network. This puts the IT department in a difficult position: users expect flexibility, and they want the IT department to be responsive to their needs. But the IT department also has to protect the data and ensure that the mobile devices accessing those data are secure if they become lost or compromised.

There is never a quick fix to a security problem, and no one knows from where the next big threat will come. To develop a secure posture, IT pros must drive security awareness throughout the entire organization. All users should use strong passwords, be careful of storing unencrypted data on laptops and mobile devices, and avoid taking large data sets from the office. From a technical standpoint, even enterprises may need expert assistance to harden their networks and track threats. Don't wait until after a security breach to take action!

*\*As reported by David Talbott*

“

*The reality is that few organizations, regardless of their size, can match the security and skills that cloud services providers can offer.*

”

# EVEN GREAT FIREWALLS CAN BE COMPROMISED



**DAVID  
FOSDIKE**

Principal IT Security and  
Forensics Consultant,  
IT Investigations

During the 1970s, David Fosdike administered and programmed IBM mainframe and later IBM and DEC midrange computers. He specialized in networking and later security. After 30 years, he moved into private security and forensic consulting. His IT security clients range from government authorities to national retail and educational organizations. He holds a master of information systems security (with distinction) degree and multiple certifications. David is active in social media on InfoSec issues and is a qualified certification instructor.

   
Twitter | Website

I deal with other people's infrastructure a lot. The problem I would put at the top of the list is people, because not only do you have people within the organization but people who are external to the organization, and they need to be either protected or protected against. There's also a big problem with management buy-in of security. Management needs to buy in in word and in deed, putting money on the table.

A company I worked for had a chief executive officer (CEO) who was going on a business trip to China. He delivered a laptop with all his information, including a five-year plan for his business, to the help desk so that the techs could install software on it. In a pocket of the laptop bag were all his passwords, including the password to unlock information about the five-year plan. If that laptop had been stolen, everything would have been compromised. A backdoor into the network would have been available.

You can only say so much to a CEO. If he's taking a company laptop on a business trip, that's part of your network. It's now separated from your network but available to get back in through a virtual private network (VPN). That's why you need management buy-in: everything needs to be encapsulated in policy.

Policy should be based on risk assessment. What are your risks? Create policies that outline your statements of intention and desired outcomes. Under that, you have procedures, work orders, and such. Policies create order and let administrators know areas of risk and how to mitigate them.

*“ Management needs to buy in in word and in deed, putting money on the table. ”*



## KEY LESSONS

- 1 EVEN AN ORGANIZATION THAT HAS GREAT SECURITY TOOLS CAN BE AT RISK IF THE PEOPLE WHO ADMINISTER AND USE THOSE TOOLS DON'T UNDERSTAND THE RISKS THEY FACE ON A DAY-TO-DAY BASIS.
- 2 SECURITY POLICIES HAVE TO HAVE CONSEQUENCES. WITHOUT THEM, THOSE POLICIES ARE NOTHING MORE THAN VAGUE THREATS.

# EVEN GREAT FIREWALLS CAN BE COMPROMISED

One thing I've found is that it's difficult to get companies to do anything with security unless they're held to it by policy. And those policies must have teeth. Banks, large organizations, and defense contractors have security that works. It works because they have policies that include punitive measures designed to ensure that requirements are met.

The next level of people are the security administrators. Those people have to take their jobs seriously, and I find that sometimes that's a problem. They're often so technology focused that they don't see the big picture. Unless you're thinking about the actual architecture of your network and your perimeter, you can end up with holes that you don't know about, even if you have a great firewall.

For example, I audited a school in a semirural area that had a Bring Your Own Device policy to allow teachers to use their own devices on school network. Unfortunately, no controls were in place around how those devices were connected to the network or what kind of antivirus they were required to have. The school also had a VPN with a very weak password, so that expanded the school's perimeter into the homes of everyone who knew that password.

People don't understand how a perimeter works, particularly how a demilitarized zone works in terms of protecting your perimeter. They open devices inside a network to the outside, not realizing that as soon as they do so that that device becomes a gateway into the rest of the network.

Any device that's connected to your network can become part of your perimeter. It's a little island of your network sitting out in the public arena. If that area is compromised, your whole network is compromised.

In the end, you have to have good technology and people who are trained in not only threat awareness but incident management. The technology is always one step behind the criminals, and law enforcement is always one step behind the technology. Unless people know how to handle threats, your technology and security policies won't be enough.

“

*Unless you're thinking about the actual architecture of your network and your perimeter, you can end up with holes that you don't know about.*

”



**SIMONE  
JO MOORE**

Senior Consultant and  
Master Trainer,  
SJM

Simone Jo Moore works internationally with multiple organizations, probing the hearts and minds of what makes business and IT tick—particularly the repartee that leads to evolution and revolution to jumpstart people's thinking, behavior, and actions at any level. Actively engaged across various social media channels, you'll find Simone sharing her more than 20 years of experience in strategic and operational business design, development, and transformation. She follows four key business principles: people connected, knowledge shared, possibilities discovered, and potential realized.

    
Twitter | Website | Blog

As an IT service management design consultant, I look to others with the relevant technical skills for the ground-level implementations. From my vantage point, however, I can identify three great challenges to enterprise application infrastructure and network security:

- **People;**
- **Understanding risk; and**
- **Understanding security's business role.**

## People

Everyone should understand the corporate IT security policy. Everyone will have read some such policy on joining the organization and know one exists. However, I generally find that they don't know much beyond the basics - such as, you shouldn't share your password or post organization information on your personal social media channels. Everyone plays a role in business security: the missing element is communication.

The focus needs to start at induction training of all new employees. Rather than just reading a policy, they must fully understand the security consequences of their role and actions. Incoming IT staff, as part of the three-month probationary period, should receive extensive and ongoing training on all network hot spots, vulnerabilities and actions to be taken if a threat arises. They must understand the flow of information through the systems and how any information released or code altered can threaten security.

“Improving communication flow, using the right channels with people and building up a culture around security's importance works wonders.”



## KEY LESSONS

- 1 **AUTOMATION IS CRUCIAL: JUST REMEMBER THAT ALL SOLUTIONS ARE HUMAN DESIGNED AND THEREFORE VULNERABLE.**
- 2 **ONGOING TRAINING AND COMMUNICATION ARE CORE NETWORK SECURITY TASKS.**



# COMMUNICATION AND CULTURE

Making that understood does not have to be all stick and no carrot, either. Improving communication flow, using the right channels with people and building up a culture around security's importance works wonders.

## Understanding Risk

Sometimes, enterprises don't understand their own attitude toward risk, so they don't assess it well. Industries like financial services are naturally risk-averse and tend to view security as a worthy investment. Some startups, in contrast, are so focused on getting to market that they gamble. Maybe that's OK, but no institution should approach security blindly.

The response to this challenge is similar to the first: it boils down to training and awareness, while improving the knowledge and ability of the people. Perform thorough risk assessments, and identify available automated solutions to assist in identifying risks. Then, determine the proper level of security investment that is desirable for your company in line with the stakeholder outcomes required.

## Understanding Security's Business Role

The IT department is there to understand, facilitate, and defend business outcomes. Yet sometimes, there is a disconnect between business requirements and IT's understanding. It is not so much that IT lacks the technology or capability to react but that there is so little understanding of the impacts of security's outcomes from the business perspective.

It is, of course, vital to implement automated solutions—password auto-resets, web application firewalls, intrusion prevention and detection, and the like. Just remember that these are human-designed tools and therefore imperfect. Go farther with your testing - some organizations hire hackers to deliberately attempt cracking into their systems, demonstrating both the latest hacker capability and the strengths and weaknesses in your systems. The results are fed back into the process loop of risk assessment and any required security improvement initiatives.

“

*Network security concerns continually flow through strategy, design, transition and operations.*

”



# COMMUNICATION AND CULTURE

Your business outcomes are impacted directly by the quality of your cyber-resilience. I strongly recommend becoming familiar with the governance and best practices outlined in various IT service management (ITSM) frameworks to bolster the organization's specific legal requirements. Look into the Control Objectives for Information and Related Technology (COBIT) and Information Technology Infrastructure Library (ITIL) frameworks. In particular, since cyber-attacks are more prevalent in today's environment, the Resilia best practice portfolio is a cross-organization approach, not just IT, and it aligns with other frameworks. It is focused on Cyber resilience - resisting, responding and recovering from attacks that will impact the information you require to do business.

Network security concerns continually flow through strategy, design, transition and operations. Put the right people, processes and technologies in place and use continual strategic improvement practices. Commit to ongoing communication and training. These tasks are core to what must be done.

“

*Go farther  
with your  
testing - some  
organizations  
hire hackers  
to deliberately  
attempt  
cracking into  
their systems.*

”

# EFFECTIVE INFORMATION SECURITY REQUIRES THOROUGH USER EDUCATION



**MATTHEW  
WITTEN**

**Information Security Officer,  
Martin's Point Health Care**

Matthew Witten has developed and led many information security, incident response, and penetration testing teams. Currently the information security officer for Martin's Point Health Care, Matthew is the former CISO for the Louisville Metro Government and the University of Louisville. He has extensive experience in information security and co-developed an incident response and risk program in wide use. Matthew holds an MBA as well as CISSP, CISA, and CRISC certifications.



My top challenge in securing our network and application infrastructure is determining what the boundaries of the network and application infrastructure are today. From an organizational standpoint, as we shift from keeping everything on premises to converting some information to the cloud, running some applications in the cloud, or actually storing data in the cloud, it's critical to make sure we secure and control that information. This is especially important because we're protecting regulated data for our health care patients and members.

It's imperative to have the right network appliances and application security solutions in place. If you don't know what's going on inside your network, you have no hope of catching it. We consider intrusion detection, intrusion prevention, or even in some cases technologies that look at east-to-west traffic. Having perimeter firewalls and antivirus in place are hugely important, too, of course, but another priority is ensuring that the weakest link is trained up. By *weakest link*, I mean the human aspect—you, me, and everybody else in the organization.

Effectively training the human element is critical, because that's frequently where an attacker will be getting in. The network security perimeter has been hardened quite a bit, so hackers often attempt to bypass it by using phishing exploits or social engineering techniques. It's unacceptable for us as security professionals to shrug and say that the users are uneducated. Our job is to ensure that they get that education. Just like we have to ensure that the firewalls are configured correctly, we have to ensure that our employees understand how to avoid risky situations or that they know to alert the right individuals when something suspicious is going on.

“It's imperative to have the right network appliances and application security solutions in place.”



## KEY LESSONS

- 1 ALONG WITH ENSURING THAT YOU HAVE THE RIGHT INFORMATION SECURITY INFRASTRUCTURE IN PLACE, YOU MUST PLACE A PRIORITY ON USER EDUCATION.
- 2 CAREFULLY EVALUATE THE UNIQUE SECURITY CHALLENGES THAT CLOUD SOLUTIONS POSE.

# EFFECTIVE INFORMATION SECURITY REQUIRES THOROUGH USER EDUCATION

I recommend conducting ongoing user training that covers issues your users may face in their personal lives. We send out newsletters that describe how users can protect themselves while shopping online, for example, right before the holiday shopping season starts. We've also done successful lunch-and-learn sessions in which we set up a lab and pretended that we were a Wi Fi hotspot at a coffee shop, then showed the attendees how easy it is to gain unauthorized access to a phone or computer in that environment. I recently joined my current organization, so I'm just starting to see the fruits of our efforts here, but one way I knew we were making a difference at my last job was when I started getting email from different users four or five times a day saying, "Hey, I got this suspicious email." That showed me that we were beginning to have some success.

By carefully evaluating the unique security challenges that cloud solutions pose, making sure that you have the right network security infrastructure in place, and proactively educating your users on the ever-evolving threats out there, you can move the needle on preventative information security at your organization. It requires no small amount of effort, but it makes a significant impact for the better.

“

*I recommend conducting ongoing user training that covers issues your users may face in their personal lives.*

”



**PETER  
SCHAWACKER**

Director, Security  
Intelligence Solutions,  
Optiv Security, Inc.

Peter Schawacker leads Optiv Security's Center of Excellence for Security Intelligence Solutions. He has been an analyst, engineer, technology evangelist, and manager in the field of information security since the late 1990s. An expert in security intelligence technologies and practice, Peter has led the creation of security operations centers for Fortune 500 companies across industries and government. He is a pioneer in the application of Agile software development practices to security products.



Website

I'm in the business of detecting attacks and understanding the nature of those attacks so that people can contain them. If I had to stack the challenges that organizations face in achieving security, I would put the lack of skilled, available labor as the biggest one; poorly implemented technologies and poorly run IT next; and poorly run security third. And really, they're all related.

The lack of skilled IT staff is just the fact that there aren't enough people to do the work that's required. The pool of labor simply can't grow quickly enough. In large part, it's because people don't have opportunities to get into the business and learn in practical ways. Or, they're mismanaged by unskilled leadership in those technologies, so you wind up wasting your security investment after the fact.

Another part of it is the IT department understanding what the business needs and leading the organization down a path that will take them there. So much of this comes down to communication. Security is all about inner-species communication among security nerds or really technical talent, the people who understand regular IT processes, and people who understand what the business is about.

*“ With every change to a product's codebase, there is the possibility of issues and the possibility of security vulnerabilities. ”*

## KEY LESSONS

- 1** BUSINESS, THE IT DEPARTMENT, AND SECURITY PEOPLE ALL NEED TO UNDERSTAND THE ORGANIZATIONAL GOALS AND WORK TOGETHER AS A TEAM TO ACHIEVE THOSE GOALS WHILE MAINTAINING A SECURE ENVIRONMENT.
- 2** DEVOPS SHOULD BE CONSIDERED FOR CREATING SMALLER, MORE FREQUENT SECURITY RELEASES; PATCHES; AND UPDATES. THESE CAN REDUCE THE NUMBER OF SECURITY ISSUES RESULTING FROM APPLICATION UPDATES.



# PEOPLE, TECHNOLOGY, AND SECURITY

The people who build and operate systems and are supposed to help the business often have no idea what the business does. But the people who are in the business don't understand IT, either. Regular IT people, like developers or systems administrators, will implement new services or change services without any regard for the security implications, which leads to system vulnerabilities. There needs to be someone—typically, business analysts or IT leaders—who can figure out how to cross boundaries between IT and business processes.

Poorly implemented technology is also an issue. In many organizations, the IT department runs poorly because of a lack of integration between functions and a tendency to do things that are too big. For example, products tend to have updates once a year or maybe once a quarter. Those product updates will include new features and bug fixes, and they'll include lots of changes. With every change to a product's codebase, there is the possibility of issues and the possibility of security vulnerabilities.

The solution is to release more frequently, with less stuff in each release. DevOps is a strategy that's increasingly being used to create more releases and reduce the cost of the release cycle itself. Because you can release more often and thereby reduce the amount of change in the releases, the results are easier to fix.

Netflix does this beautifully. It's a sophisticated, very mature organization when it comes to DevOps. Then, you have most of the world, which is backwards and still trying to do things as if they were hoping that mainframes would come back. To break this cycle, security managers need to show business and IT leadership the value of small, frequent releases and standardization. One way to do that is to introduce these leaders in forums, where they can compare notes and see that another world is possible.

“

*Security managers need to show business and IT leadership the value of small, frequent releases and standardization.*

”





# PEOPLE, TECHNOLOGY, AND SECURITY

The last issue is poorly run security programs. There is the necessity to maintain technologies after implementation. For example, we have many customers that will invest heavily in the purchase and installation of security tools like firewalls. Unfortunately, those companies make heavy investments in the security program, but then they don't maintain or continue to develop those technologies. The tools just rot on the vine, leaving the organization unable to respond to threats as they happen and unable to integrate IT systems in ways that are secure.

Organizations need to simplify operations. They need to simplify IT environments. They need to reduce the variety and diversity of systems and tools so that there are fewer changes that are easier to manage. Firewalls can reduce the amount of noise by simplifying and normalizing the amount of network traffic that goes in and out of a network. They can also reduce the kinds of network traffic that passes through your network perimeter. The fewer things you pass through and the more standard your application programming interfaces, the less you have to think about and the smaller your attack surface.

“

*Then, you have most of the world, which is backwards and still trying to do things as if they were hoping that mainframes would come back.*

”



**SCOTT  
STEWART**

Director, Technology  
Advisory,  
Deloitte

Scott Stewart is a director within the Technology Advisory Practice at Deloitte focused on CIO advisory, IT strategy, and sourcing strategy. Based in Australia, Scott has delivered IT consulting services to many multinational organizations in the Asia Pacific region, the Middle East, and the United States. Scott is a seasoned ICT executive, having been a CIO for many years in the financial services sector as well as an acclaimed senior industry analyst and research director.

 |  |  | [Twitter](#) | [Website](#) | [Blog](#)

A client of mine recently discovered that a competitor had breached the client's network. For an extended period, outsiders were freely accessing the client's proprietary sales information.

It came as quite a shock. Members of the client organization thought they had done everything right by investing time, money, and thought into perimeter security, tools, and processes. Unfortunately, they neglected the "people" aspect of security. By that, I mean social engineering, which is the trick hackers use to crack into networks by manipulating naiveté and the natural human impulse to be trusting. It is one of the most commonly used network-infiltration tactics.

It seems most likely that someone inside the organization facilitated the competitor's access in a way that was difficult to detect let alone prove. Afterward, my client closed the gap in its processes and dealt with some of its people issues, but it learned the key lesson the hard way. When it comes to security, you can never be too prepared.

We tend to view security through the lens of technology and process, but in so doing, we too easily overlook the pivotal role of the human factor in the security value chain. What are the best ways to head off that problem?

- **Awareness.** Awareness is the number one defensive measure. Make sure your employees understand the social engineering threat. It is also important that you stay up-to-date on evolving social engineering techniques and trends. Perpetrators constantly reinvent themselves.

“ For an extended period, outsiders were freely accessing the client's proprietary sales information. ” 

## KEY LESSONS

- 1 SOCIAL ENGINEERING IS PERHAPS YOUR GREATEST NETWORK SECURITY VULNERABILITY.
- 2 BEING GOOD TO EMPLOYEES IS A NOT INSIGNIFICANT PART OF AN AIRTIGHT SECURITY BATTLE PLAN.

# SOCIAL SECURITY

- **Engage the whole of business.** Security is not only the job of your IT staff. Your security-awareness campaign should not fail to include your executives. These self-professed “luddites” may be your greatest danger and vulnerability.
- **Follow a disciplined strategy.** If you don’t have a strategy, find one. I have my clients start with the four steps to cyber security, as outlined in Deloitte’s 2014 handbook, [Cyber Security: Empowering the CIO](#), which directs them to follow a more disciplined and structured approach.

At a high level, the four steps the handbook outlines include:

- **Being prepared.** This is the strategy of achieving “security through vigilance and resilience.” It involves establishing a process of monitoring, planning and testing, response, and insurance.
- **Setting the bar.** This is the strategy of achieving “security capability by design.” It involves establishing a risk-based and business-aligned security strategy, identifying and protecting valuable assets, and aligning architecture to ensure that a security strategy can be achieved.
- **Getting the basics right.** This is the “security by control” step. It includes setting access protocols, conducting regular patching, managing vulnerable files, securing essential systems, and conducting regular testing and root cause analysis.
- **Establishing personal protection.** Deloitte describes this as “security through behavior”—cultivating continued security awareness, leading from the top, and making clear the consequences of bad behavior. It also encourages the adoption of security practices at home.

Deloitte’s handbook is based on the premise that executives and board members must have “skin in the game” as it relates to cyber security. Corporate officers are every bit as responsible to stakeholders as the chief information officer.

A final thought: I’d invite you to mull over one additional element of the human factor as it relates to data and network security. A bad management style can create a disgruntled employee; that person might quickly be transformed from a loyal worker into a data-security threat. Likewise, an underpaid, underappreciated staffer might give in to temptation and hand over data in a bid to curry favor with your higher-paying competitor. My point is that by being a good leader and people manager, by being good to your people, you are contributing a not insignificant element to a holistic data and network security strategy.

“

*Corporate officers are every bit as responsible to stakeholders as the chief information officer.*

”

# In cybersecurity, there's the slick SALES PITCH...

...and then there are facts.

**Our focus on innovation** over the last 15 years means you can simplify your security strategy and stay ahead of the threat today—not in an upcoming version that only exists in a pitch over golf.

We deliver a consolidated approach from datacenter to endpoint, plus global visibility and control on one OS with one management console.

**It's because we like our labs more than the golf course.**

Get a Cyber Threat Assessment today and get the facts about your security posture.

[www.fortinet.com/ctap](http://www.fortinet.com/ctap)

**FORTINET**®

**99%** effective breach detection

**5X NGFW** performance

**#1 unit share** worldwide in network security

**Over 200** zero-day attacks discovered



Data Center Firewall  
Next Generation Firewall  
Breach Detection  
Web Application Firewall

Security Without Compromise