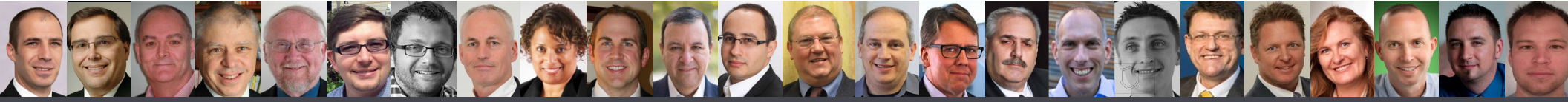

Mighty Guides

Securing Your Network and Application Infrastructure

Part 1: Building and Executing a Plan for Your Network Security

8 Experts Share Their Secrets

SPONSORED BY:

FORTINET®

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, not just the methods of access.

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.

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 midsized 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

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.

Building and Executing a Plan for Your Network Security

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.

97.3% effective breach detection

5X NGFW performance

#1 unit share worldwide in network security

Over 200 zero-day attacks discovered

Get a Cyber Threat Assessment today and get the facts about your security posture.
www.fortinet.com/ctap

FORTINET®

Security Without Compromise

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.

Twitter | Website | Blog

Download the full eBook:
Securing Your Network and Application Infrastructure

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.

> *"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

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.

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.

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

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.

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

Download the full eBook:

Securing Your Network and Application Infrastructure

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.

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.

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.

> *"When choosing the right network security appliances and application security solutions, your company must first understand its needs."*

STRENGTHENING INFORMATION SECURITY: A LONG-TERM PROCESS

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 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."

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

Download the full eBook:
Securing Your Network and Application Infrastructure

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.

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.

> *"If you don't see what's going on, then small threats become major issues."*

People mention that with FortiGate, for example, adding troubleshooting and network testing features to the UI would be useful.

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.

"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.

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

Download the full eBook:
Securing Your Network and Application Infrastructure

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."*

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

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?

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."*

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.

- **97.3%** effective breach detection
- **5X NGFW** performance
- **#1 unit share** worldwide in network security
- **Over 200** zero-day attacks discovered

Get a Cyber Threat Assessment today and get the facts about your security posture.
www.fortinet.com/ctap

FORTINET®

Security Without Compromise

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.

Twitter | Website | Blog

Download the full eBook:
Securing Your Network and Application Infrastructure

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.

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.

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.

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

TOO MANY SOLUTIONS, NOT ENOUGH ANSWERS

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.

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.

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

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.

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

Download the full eBook:
Securing Your Network and Application Infrastructure

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.

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.

> *"There's a shortage of the skill sets required in this line of work."*

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. 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.”

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

Download the full eBook:
Securing Your Network and Application Infrastructure

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.

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.

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.

> *"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."*

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. 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 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.

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

Download the full eBook:
Securing Your Network and Application Infrastructure

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.

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:

> *"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."*

DON'T FORGET THE BASICS

- **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.
- **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.

"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."

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.