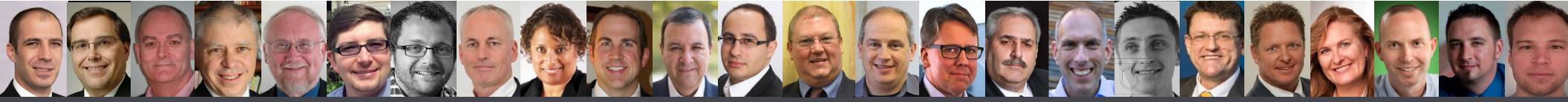

Mighty Guides

Securing Your Network and Application Infrastructure

Part 5: The Human Factor and a Culture of Security

6 Experts Share Their Secrets

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.

The Human Factor and a Culture of 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

SECURITY IS A TECHNICAL AND A HUMAN PROBLEM

MICHAEL KRIGSMAN

Industry Analyst and Founder,
cxotalk.com

The founder of cxotalk.com, Michael Krigsman 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

Download the full eBook:
Securing Your Network and Application Infrastructure

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.

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 midsized 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.

> *"Network security has become extremely complex because networks have become more complex."*

SECURITY IS A TECHNICAL AND A HUMAN PROBLEM

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.

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

Download the full eBook:
Securing Your Network and Application Infrastructure

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.

> *"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

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.

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.

> *"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."*

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.

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

Download the full eBook:
Securing Your Network and Application Infrastructure

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.

> *"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.

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.

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.

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

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.

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.”

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

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.

Twitter

Download the full eBook:
Securing Your Network and Application Infrastructure

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.

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.

> *"It's imperative to have the right network appliances and application security solutions in place."*

EFFECTIVE INFORMATION SECURITY REQUIRES THOROUGH USER EDUCATION

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.

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

Download the full eBook:
Securing Your Network and Application Infrastructure

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.

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.

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

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.

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."

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

Download the full eBook:
Securing Your Network and Application Infrastructure

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.

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?

> *"For an extended period, outsiders were freely accessing the client's proprietary sales information."*

- **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.
- **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.

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

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

> *"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."*