



Securing Your Network and Application Infrastructure

Quotes from 24 Experts



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.



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.

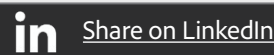
Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

© 2015 Mighty Guides, Inc. | 62 Nassau Drive | Great Neck, NY 11021 | 516-360-2622 | www.mightyguides.com



**SHAWN
E. TUMA**

Partner,
Scheef & Stone, LLP



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

You can't protect what you don't even know you have. To that end, you must undertake four crucial tasks: thoroughly understand the data your organization has, assess threat vectors and external access points, put automated security systems in place, and have a solid breach response plan in place. Cover the basics, and a breach won't catch you by surprise.



Want to read more?
[Download the full eBook Free >](#)

About the Author: 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.




**ERIC
VANDERBURG**

Security Executive, Author,
Cybersecurity Investigator, and
Expert Witness



 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

Securing your network and application infrastructure is a long-term process. In addition to determining the right technology and controls, you must assess the cost associated with the disclosure of sensitive information and train the people who use the system to observe security protocols, such as strong passwords and access controls. It's important to identify the right solution, but the human element is equally critical.




Want to read more?
[Download the full eBook Free >](#)


About the Author: 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.



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



 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

To know what's going on in your organization, you need a single pane of a glass—an administrative interface that connects all the security elements in your organization. Combined with stability and the ability to support mobile devices, these features form the cornerstone of the security solutions you choose for your organization. Crowd-sourced review sites made up of unbiased security professionals can point you in the right direction.



Want to read more?
[Download the full eBook Free >](#)


About the Author: 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.



**NIGEL
FORTLAGE**
Vice President, IT,
GHY International



 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

The two greatest security challenges we face are the speed and variation of innovative new attacks and the complexity of our infrastructure. 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.



Want to read more?
[Download the full eBook Free >](#)


About the Author: 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.



**PATRICK
PETERSON**
CEO and Founder,
Agari

 |  | 
Twitter | Website | Blog

 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

It's hard to secure your enterprise when the front door is wide open. Organizations today are spending so much time responding to immediate threats that they don't have time to solve the underlying problems. The key to addressing this issue is to select solutions that have strong application programming interface (API) capabilities and develop security staff who make decisions based on business needs.



Want to read more?
[Download the full eBook Free >](#)


About the Author: 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.



**DAN
TWING**
President and COO,
EMA


 |  | 
Twitter | Website | Blog

 Tweet this Quote

 Share on LinkedIn

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

Organizations everywhere face a shortage of skilled IT security staff. Coupled with the abundance of legacy applications still in operation, the proliferation of mobile workers and remote offices, and the lack of effective change control, companies run the risk of opening security holes with each change they make. With good analytics, however, organizations have a much better chance of managing security incidents.



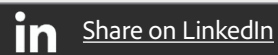
Want to read more?
[Download the full eBook Free >](#)

About the Author: 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.



**DAVID
HARLEY**

Senior Research Fellow,
ESET



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

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. Ideally, an organization will recognize the need to build a more secure infrastructure before a security breach has occurred. By implementing a security initiative as a team effort, even a relatively small security project can have broad implications.

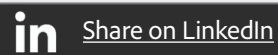


Want to read more?
[Download the full eBook Free >](#)

About the Author: 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.



**RYAN
DEWHURST**
Senior Research Fellow,
Dewhurst Security



“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*. ”

The greatest and potentially most devastating security challenges are the most basic ones. Three essentials can put you ahead of the game, though: encourage your employees to use strong, secure passwords; keep the company software up-to-date; and test your software—both the applications you develop in house and those purchased from third parties.



Want to read more?
[Download the full eBook Free >](#)


About the Author: 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.



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

 |  | 
Twitter | Website | Blog

 Tweet this Quote

 Share on LinkedIn

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

In providing electronic billing services to clients, two of the greatest security concerns are managing hosting vendors whose services we use and managing inadvertent or accidental breaches by staff. To that end, look for vendors that are open with you and flexible in addressing action items, and take every opportunity to identify weaknesses, strengthen training, and improve policies for staff.



Want to read more?
[Download the full eBook Free >](#)

About the Author: 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.



**JOHN
MADDISON**

Vice President, Marketing,
Fortinet, Inc.


 
Website | Blog

 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

The greatest vulnerability for many businesses, especially mid-sized companies, is data, whether it is unique intellectual property or simply data that enable daily operations. One strategy more and more companies are employing is securing the internal network from within by segmenting the core network, breaking it down by users, applications, or traffic. If the network is protected, the people and devices that connect to it will be better protected, as well.





Want to read more?
[Download the full eBook Free >](#)

About the Author: 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.




**ROBERT
SHULLICH**

Enterprise Security
Architect,
AmTrust Financial Services

 
Twitter | Website

 [Tweet this Quote](#)

 [Share on LinkedIn](#)

“ Many organizations lack inventories of assets. The reality is, you can't protect what you don't know you have. ”

The danger businesses face every day can be summed up in one sentence: the organization's security person needs to get it right every hour of every day, while the data thieves need to get it right only once. To even the playing field a bit, companies must know what their assets are. Only through situational awareness can organizations defend themselves against today's cyber-criminals.



Want to read more?

[Download the full eBook Free >](#)


About the Author: 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.



**DAVE
WATERSON**
CEO,
SentryBay

 |  | 
Twitter | Website | Blog

 Tweet this Quote

 Share on LinkedIn

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

Today's companies realize that it's not a matter of *whether* they will get breached but *when*. That's why procedures and rapid response teams—in addition to technical solutions—need to be in place. Only when the focus of enterprise network security shifts closer to the enterprise's core, its data, can you stay ahead of potential attackers.



Want to read more?
[Download the full eBook Free >](#)

About the Author: 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.




LINDA
CURETON

Former CIO,
NASA



 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

Companies tend to focus on protecting their perimeter. They often put so many resources into doing so that they neglect the data itself. True security requires a layered defense of several solutions, put together to give you the protection your specific organization needs. In the end, there is no one-size-fits-all solution to security.



Want to read more?

[Download the full eBook Free >](#)

About the Author: 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.




**TOM
ESTON**

Manager, Penetration
Testing,
Veracode

  
Twitter | Website | Blog

 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

Most corporate security breaches start with social engineering tactics. These approaches, coupled with vulnerabilities in company applications and misconfigured systems, make attacks easier than they might otherwise be. To lower the risk of such infiltrations, stage your own social engineering tests so that your employees know what such attacks look like—and what to do when they occur.



Want to read more?

[Download the full eBook Free >](#)

About the Author: 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.




**STEVEN
WEISKIRCHER**

Chief Information Officer,
ThinkGeek, Inc.

 
Twitter | Website

 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

External predators, internal threats, and crumbling network boundaries are major concerns for corporate security people. Help minimize the risk to your organization by using advanced technologies, conducting regular threat assessments, and running penetration tests and vulnerability assessments. In the end, security will always be a combination of advanced technology and smart people.



Want to read more?
[Download the full eBook Free >](#)

About the Author: 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.



**WILL
LEFEVERS**

Lead Information Security
Architect,
Constant Contact



Twitter



Tweet this Quote



Share on LinkedIn

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

One of the greatest challenges organizations face today is finding good technology security talent. No matter their education or certifications, nothing but experience can teach people how to respond in the moment when their organization has been breached. IT departments need people versed in the latest developments in hacker subculture, people who will run *toward* the fire, not *away* from it.



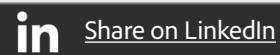
Want to read more?
[Download the full eBook Free >](#)

About the Author: 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.




**MIKHAEL
FELKER**

Director of Information
Security,
VC backed eCommerce



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

The 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. So, it is more important than ever to involve information security professionals at the earliest stages of business projects to minimize risk and project rework.



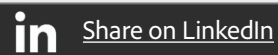
Want to read more?
Download the full eBook Free >

About the Author: 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.




**ERLEND
OFTEDAL**

Senior Security Consultant,
F-Secure



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

No matter how many protections we build into our infrastructure, we will always have vulnerable systems. Legacy applications are inherently vulnerable, users do things they shouldn't, and developers make mistakes, all of which make it that much easier for attackers to breach your systems. The best protection against such threats is early detection and rapid response through active security monitoring.



Want to read more?
[Download the full eBook Free >](#)

About the Author: 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.




**MICHAEL
KRIGSMAN**

Industry Analyst and
Founder,
cxotalk.com


  
Twitter | Website | Blog

 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

Security is a challenge for all businesses, regardless of their size. Both human and technical forces compound security issues. As networks have increased in complexity, so have the security challenges facing them. To develop a secure posture, IT pros must drive security awareness throughout the organization.




Want to read more?
[Download the full eBook Free >](#)

About the Author: 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.




**DAVID
FOSDIKE**

Principal IT Security and
Forensics Consultant,
IT Investigations

 
Twitter | Website

 Tweet this Quote

 Share on LinkedIn

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

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. That's why you need management buy-in. Everything needs to be encapsulated in policy, and that policy should be based on risk assessment and carry consequences for noncompliance.



Want to read more?

[Download the full eBook Free >](#)

About the Author: 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.




**SIMONE
JO MOORE**

Senior Consultant and
Master Trainer,
SJM

  
Twitter | Website | Blog

 Tweet this Quote

 Share on LinkedIn

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

Building your corporate communications and culture around the importance of security can work wonders in fending off attacks on your corporate network infrastructure. By requiring ongoing training and open communications among your staff and employing automation wherever feasible, you put in place the core of your security policy.



Want to read more?

[**Download the full eBook Free >**](#)

About the Author: 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.



**MATTHEW
WITTEN**

Information Security Officer,
Martin's Point Health Care



Tweet this Quote



Share on LinkedIn

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

As companies shift from keeping everything on premises to converting information or applications to the cloud, it's critical that they secure and control that information. So, it's imperative that organizations have the right network appliances and application security solutions in place, and then train their users to recognize security issues they may face.



Want to read more?

[Download the full eBook Free >](#)

About the Author: 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.

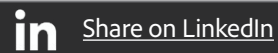


**PETER
SCHAWACKER**

Director, Security
Intelligence Solutions,
Optiv Security, Inc.



Website



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

Three of the biggest challenges organizations today face are lack of skilled, available labor; poorly implemented technologies and poorly run IT; and badly run security. By implementing DevOps principles—smaller, more frequent security releases and updates—organizations can reduce the number of security issues that results from application updates and help maintain a secure environment.



Want to read more?

[Download the full eBook Free >](#)

About the Author: 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.




**SCOTT
STEWART**

Director, Technology
Advisory,
Deloitte



 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

A company can invest time, money, and thought into perimeter security, tools, and processes, but if it neglects the “people” aspect of security—that is, social engineering, which is the trick hackers use to crack into networks by manipulating naiveté and the natural human impulse to be trusting—your organization will remain open to attack. Educated employees are essential to an airtight battle plan.



Want to read more?
[Download the full eBook Free >](#)

About the Author: 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.