PLUS: ANTIMALWARE SUITES

INFORMATION SECURITY®

OCTOBER 2011

Secure payment ecosystem

Computer security literacy

National cybersecurity

Security awareness

Tabletop exercises

Vulnerability management

Community participation

SECURITY 7 AWARD *winners*

B-SIDES ELEFANT JACOBSON
LANGEVIN PAIDHRIN TODD WISHNOUSKY

TechTarget

INFOSECURITYMAG.COM

FROM OUR SPONSORS

RSA CONFERENCE 2012
FEBRUARY 27 – MARCH 2 | MOSCONE CENTER | SAN FRANCISCO

contents

OCTOBER 2011
VOLUME 13 NUMBER 8

FEATURES

DEPARTMENTS

ALSO

What's Your Acceptable Level of Risk?

(It's Lower than You Think)

Because malware is pervasive and advanced, visiting even popular websites can be risky. But to be relevant and efficient, businesses rely on Web 2.0 sites such as Facebook and Twitter. How can you get the access you need without raising your level of risk? With the most accurate malware detection available, the M86 Secure Web Gateway protects from threats that elude other security solutions, so you can use the Web with confidence.

To learn more about the M86 Secure Web Gateway, visit **www.m86security.com/swg** today. Or call **888.786.7999** for a free product evaluation.

M86™ SECURITY
Real Time Security for the Borderless Network

Security Standouts

This year's Security 7 Award winners represent a bright spot in an industry beset by bad news. BY MARCIA SAVAGE

THIS YEAR HAS been a tough one for security, to say the least. From the RSA security breach and the subsequent attacks on defense contractors Lockheed Martin, Northrop Grumman, and L-3 Communications, to the ongoing attacks by Anonymous and the certificate authority breaches, it's been one downer after another for the industry.

But more negative news isn't the focus here. Our focus is on the positive: An industry filled with a lot of dedicated, super-smart and creative people. Each fall, we choose outstanding information security professionals in seven vertical markets to receive our Security 7 Award. After seven years, the honor roll of winners is filled with industry leaders and luminaries, including Gene Spafford, Dorothy Denning, Dave Dittrich, Mark Weatherford, Melissa Hathaway, and Chris Hoff.

This year's winners represent a diverse mix of talent, including an educator, a congressman, and a trio of security pros who created a new venue for industry collaboration. The winners have individual focuses, whether it's securing the payment ecosystem, expanding data security education to the masses or improving private-public information sharing, but they all share a common trait: tireless dedication to cybersecurity.

Our focus is on the positive: An industry filled with a lot of dedicated, super-smart and creative people.

Beginning on page 20, you can hear about their projects, passions and ideas for meeting today's security challenges. We're pleased to add to our Security 7 honor roll: Steven Elefant, formerly of Heartland Payment Systems, Douglas Jacobson of Iowa State University, Rep. Jim Langevin (D-R.I.), Christopher Paidhrin of PeaceHealth Southwest Medical Center, Matthew Todd of Financial Engines, Brian Wishnousky of Rogers Communications, and Mike Dahn, Jack Daniel, and Chris Nickerson of Security B-Sides conferences.

Four years ago, we began inviting our winners to write an essay on an information security topic they felt deeply about. This has proven to be a winning formula, producing one of my favorite issues each year. It's a treat to hear from security leaders in their own words, and one we value highly. You should too.

This year marks the first time we've given a Security 7 to an elected official, a departure from the ranks of security professionals. Over the years, information security professionals have been frustrated with the spotty attention paid to cybersecurity in Washington D.C. Every so often, we hear a lot of bluster from federal officials about the need to improve cybersecurity, but see little action. Rep. Langevin, on the other hand, has proven his continued dedication over the years, with his work on the Congressional Cybersecurity Caucus (which he created in 2008 with Rep. Michael McCaul R-TX), holding multiple cybersecurity hearings as chairman of the Subcommittee on Emerging threats, Cybersecurity and Science and Technology, and introducing legislation such as the Homeland Security Network Defense and Accountability Act. Langevin has worked hard to keep information security on the national agenda and deserves industry recognition.

2011 also is the first year we've awarded Security 7 to a group effort. Two years ago, Mike Dahn, Jack Daniel, and Chris Nickerson created an alternative to mainstream security conferences with Security B-Sides. Since the first event in Las Vegas, B-Sides has grown spectacularly, with an astonishing 40 events worldwide. By providing a way for security professsionals to come together minus the vendor booths, B-Sides has fostered invaluable industry collaboration and innovation.

Other winners are tackling core enterprise security issues of security awareness, vulnerability management and crisis planning. Their essays are illuminating and instructive.

The energy, drive and creativity of our Security 7 winners are a shining example of what's right in an industry that gets more than its fair share of negative attention.›

Marcia Savage is editor of Information Security. *Send comments on this column to feedback@infosecuritymag.com.*

We're paranoid as well. We just call it prudence. Backed by every major security certification, we can help design and install the right security solutions for you.

Trust no one except us at CDW.com/security

CDW PEOPLE WHO GET IT™

Medical Devices: The New Security Battleground

Networked medical devices introduce new risks but does a new standard go far enough in addressing the problem?

BY JOSEPH GRANNEMAN

UP UNTIL NOW, the information security risks involved with medical applications had to do with privacy breaches of patient or billing information. There was the potential of an incorrectly entered data element or an element that was not sent correctly through a medical interface. HIPAA was enacted to ensure privacy and security risks were identified and managed, although some question its effectiveness.

Today, the emergence of medical devices directly on a network introduces a new type of risk that hasn't been seen before in health care information technology. As electronic medical records systems have been quickly adopted—spurred by the American Recovery and Reinvestment Act of 2008—organizations developed a need to have certain patient data entered directly into the electronic medical record. The overwhelming task of entering all of the data was falling on clinicians, which could introduce human error into the process. As a result, medical equipment has started to sprout network jacks and wireless radios. Using the network, medical equipment can transfer patient information directly into an electronic chart, increasing clinician productivity and data accuracy.

However, a malfunction in these new types of networked medical devices could cause harm to a patient. IV pumps, respirators and other types of networked medical equipment are now reliant on the security and stability of the network they are operating on; they are basically networked computers with the same type of vulnerabilities that exist with other networked computers. These networked medical devices are susceptible to network outages, malware and even malicious access. The threat was highlighted at the Black Hat conference in July, when a security researcher reportedly demonstrated how he could remotely disable his insulin pump.

A new ISO standard, IEC 80001-1, and the accompanying guidance published in IEC 80001-2 and IEC 80001-3, have stricken the first blow in the battle for medical device security. Given how badly this standard was needed, does it accomplish what it set out to do? Like all security frameworks, the answer is dependent on the implementation specifics.

The overriding theme in IEC 80001-1 revolves around establishing a risk management program for networked medical devices. There is nothing surprising about the risk man-

agement focus as all major security frameworks embrace this methodology in one way or another. However, what is surprising is how the responsibility for securing these medical devices falls mainly on what the standard defines as health care delivery organizations (HDOs). "This requirement makes it clear that the ultimate responsibility for compliance with the standard lies with health care delivery organizations using the medical device network, irrespective of what suppliers provide," the standard states.

This stance seems reasonable at first glance because the safety and security of the network is ultimately the responsibility of the HDO. However, since the HDO has no direct input into the initial design of each medical device, the only alternative is to bolt on security measures after the fact. This is never a fully effective method, as most security practitioners can attest. The standard does require the manufacturer to disclose potential risks to security and patient safety and provides guidance on secure configurations. It also requires a contract called a Responsibility Agreement for making this disclosure, yet the contract seems more focused on protecting the intellectual property of the manufacturer. Delivering robust and secure networked medical devices has to be the responsibility of the manufacturer in order for IEC-80001 to be effective.

IEC 80001 calls for each HDO to assign an employee into a new role that will be responsible for managing the risk associated with the medical network. This role could be rolled up to an employee charged with HIPAA security as many of the goals are the same. However, the standard doesn't list qualifications for the staff member charged with this responsibility, which also is a weakness in HIPAA regulations. Many organizations have simply assigned the HIPAA security role to a PC technician with little security experience. IEC 80001 could suffer the same fate if the medical IT network risk manager does not have the appropriate background. This problem is compounded further for small medical practices that may only have few employees.

Despite its weaknesses, IEC 80001 is a much needed standard whose time has come. Patients shouldn't have to worry about injury from networked medical devices due to information security vulnerabilities or network instabilities. It starts to lay a solid foundation that with a few changes could provide the safety we all expect when we seek medical care. It's a voluntary standard at this point, but many health care quality organizations will most likely merge it into their overall safety and quality audits. There is still time for the manufactures of these networked medical devices to take the lead by integrating security practices into the design of their products. Health care providers need to take heed and recognize that these devices could pose a threat to their patients and fast-track a risk management program. It's simply the right thing to do.›

Joseph Granneman, CISSP, has over 20 years in information technology and security with experience in both healthcare and financial services. He has been involved in the Health Information Security and Privacy Working Group for Illinois, the Certification Commission for Health Information Technology (CCHIT) Security Working Group, and is an active InfraGard member.

TODAY'S CYBERCRIME IS WORLD CLASS.

ARE YOU UP TO THE CHALLENGE?

HP ArcSight Express instantly alerts you to the complex threats faced by organizations by correlating millions of events occurring across the enterprise.

For more information go to www.hpenterprisesecurity.com.

ENTERPRISE SECURITY

ANALYSIS | INTERNET SECURITY

Broken Trust

Certificate authority breaches prompt calls for Internet security alternatives. BY ROBERT WESTERVELT

THIS SUMMER'S ATTACK on Dutch certificate authority DigiNotar has prompted browser makers to stop accepting the firm's digital certificates and fueled a renewed interest in finding a replacement for the fragile Internet digital certificate infrastructure.

DigiNotar's security practices and technologies were woefully inadequate, according to Dutch security firm Fox-IT, which conducted an audit of its systems. The certificate authority, which sells commercial secure socket layer (SSL) certificates and works with the Dutch government on its PKI implementation, received a hail of criticism when it announced Sept. 5 that a hacker had breached its systems and stole several SSL certificates.

The breach actually occurred July 19; DigiNotar thought it had quietly revoked all fraudulent certificates afterwards. But the compromise of the company's CA servers came to light when security researchers discovered DigiNotar had issued a valid SSL wildcard certificate for Google to an Iranian-based entity. The rogue Google certificate is believed to have been used to monitor Gmail messages in that country. A wildcard certificate helps enable SSL encryption on multiple sub-domains using a single certificate.

"With the way this was handled and all the previous issues we've had with the certificate authority infrastructure, the implied trust of SSL is currently questionable if you haven't fully patched," says Paul Henry, security and forensic analyst at Scottsdale, Ariz.-based vulnerability management vendor Lumension Security. "In light of the failures we're seeing here, we can be looking at very serious issues, so we should absolutely be looking at alternatives to the system we currently have."

Security experts say the compromise of DigiNotar and the similar attack on certificate authority Comodo in March erode the trust inherent in digital certificates and tarnishes the CA system altogether. Chester Wisniewski, a senior security consultant with Sophos, says the problems should be top-of-mind at enterprises because many organizations use digital certificates to authenticate users for SSL VPNs, the company intranet and e-com-

merce systems. Organizations using Web applications, such as Salesforce.com and other services, also use digital certificates.

"SSL has multiple components to it and this is about the authenticity of validating [who] you are talking to on the Internet," says Wisniewski. "Right now we're forced into relying on this broken system, so any alternatives must be considered."

One alternative validation method under development is the Perspectives Project, led by Dan Wendlandt and maintained by Carnegie Mellon University. Wendlandt says the problems with digital certificates have been well documented. For example, researchers in 2008 demonstrated a way to construct a rogue certificate authority and issue digital certificates.

"For a long time, weaknesses were considered theoretical and we were accused of fear mongering," Wendlandt says. "With certificate authorities, if anyone gets these magic keys, they can spoof the server that a certificate is valid and that's a scary thing."

"With certificate authorities, if anyone gets these magic keys, they can spoof the server that a certificate is valid and that's a scary thing."

–DAN WENDLANDT,
Perspectives Project, Carnegie Mellon University

Under the Perspectives Project, public notary servers are used to validate SSL certificates. It bypasses certificate authority approval and instead the servers check for consistency of the certificates used by the network over time. The project enables users to pick what group of network notary servers they trust or users can accept the defaults in the Mozilla Firefox plugin.

At the DEFCON hacker conference in August, noted security researcher Moxie Marlinspike unveiled an alternative system called Convergence, which builds on the Perspectives Project. The notary system uses network probing from various locations to determine the validity of websites.

The power to change the current system, says Lumension's Henry, is with the browser makers who need to build-in support for alternative methods. Convergence currently is in use as an extension for Mozilla Firefox users. Google, according to Wendlandt, is considering adding similar functionality in Chrome.

"We truly feel that this was fundamentally the wrong way to build a security system," says Wendlandt of the current CA architecture. "Internet security is a very important and personal so building a better system that can be trusted and doesn't impact privacy is where we need to go."

Robert Westervelt is the news director of SearchSecurity.com. Send comments on this article to feedback@infosecuritymag.com.

In the Crosshairs by *Information Security* staff

Android devices are becoming more widespread and so is Android malware. Devices running the Google Android platform have become the most popular group of targets for mobile malware developers, outpacing Java Micro Edition and Symbian platforms, according to a report issued by McAfee. Security researchers have identified Android malware with botnet functionality and rootkit features. This summer, Trend Micro researchers discovered an Android Trojan capable of recording phone calls and SMS messages, and Symantec researchers documented a high-profile Android app that was compromised and bundled with a Trojan.

Mobile malware samples:

Q2 2009 – 600

Q2 2010 – 900

Q2 2011 – 1,200

Number of new malware samples targeting the Android platform in Q2 2011: 44

Number of new malware samples targeting Apple's iOS platform: None

SOURCE: McAfee

Number of criminal command-and-control infections of Android devices in the first six months of 2011:

40,000

SOURCE: Damballa

overheard

"The fact that you can get apps from anywhere with the Google Android platform–what we call provenance–definitely puts the platform more at risk."

–JOHN HARRISON, group manager for Symantec Security Response

Finally. A Better Way To Audit Activity On Any Server.

Centrify DirectAudit records and replays privileged user sessions on UNIX, Linux and Windows servers. There's never been a better way to know if your IT contractors and outsourced staff are solving problems … or creating them.
Download DirectAudit now at centrify.com/windowsaudit

Download DirectAudit at centrify.com/windowsaudit

Centrify®

Determining the Value of Information Security Certifications

An InfoSec Leaders survey examines the impact of different certs on the security profession. BY LEE KUSHNER

CERTIFICATIONS AND CERTIFICATION BODIES have played a prominent and controversial role in the development of the information security profession. Attaining certifications has been viewed as a common method to create a personal brand of credibility and knowledge. For many, the effective leveraging of this brand has led to the establishment and the advancement of their information security career. This impact has not gone unnoticed, and the certification industry has become a lucrative business.

Certification and educational bodies that offer training have been able to capitalize by developing a large number of programs that appeal to every segment of the profession. If you include all of the encompassing information security certification programs (i.e. CISSP, CISM, etc), the 24 SANS GIAC certifications programs, and vendor-based certifications (i.e. RSA, Symantec, etc), there are more than 50 options. It can be argued no organization has been more effective in marketing certifications than ISC(2), and its CISSP; as of August, ISC(2) confirmed there are 76,335 active CISSPs worldwise, almost double the number of SANS/GIAC certified security professionals. ISC(2) claims on its website that by holding the CISSP, you will have "higher earning potential," "expanded career opportunities" and "join an elite network;" it is no wonder that this certification is the most popular.

With messages of this strength, and the corresponding numbers to support it, how are information security professionals expected to respond? Do non-certified information security professionals have any chance in achieving career success? By not holding information security certifications, are your career opportunities limited? Is your earning potential forever

Lee Kushner's and Mike Murray's blog can be found at www.infosecleaders.com where they answer your career questions every Tuesday, or you can contact them via email.

Lee Kushner is the president of LJ Kushner and Associates, an information security recruitment firm, and co-founder of InfoSecLeaders.com, an information security career content website.

Mike Murray has spent his entire career in information security and currently leads the delivery arm of MAD Security. He is co-founder of InfoSecLeaders.com, where he writes and talks about the skills and strategies for building a long-term career in information security.

diminished? Exactly how elite are networks that boast such large numbers? What is the value of information security certification?

To find out, infosecleaders.com launched an independent survey that was open to all information security professionals, and promoted through the media, conference presentations, and social media. The survey polled those holding information security certifications, those not holding information security certifications, and those holding the CISSP. In total, there were 1,349 respondents to the survey, of which 1,000 held at least one information security certification. Fifty-two percent of the respondents (699) either currently hold (667) or had once held (32) the CISSP certification.

CERTS AND A FALSE SENSE OF SECURITY

Some of the most revealing findings focused on topics that included access to employment opportunities, return on investment, motivation for certifications, and attitudes toward the certification bodies. In addition, by addressing questions to different subsets of the respondents, it was particularaly revealing to see how perceptions differed on these topics, depending on the respondent's certification status and particular point of view. Looking at the collected data, through my lens as an information security executive recruiter, provided an interesting contrast of perception and practice.

While certifications may indeed provide you with access to opportunities, they are a long way from guaranteeing you will be hired.

One of the best examples of this difference in perception among non-certified and certified information security professionals focuses on access to job opportunities. Fifty percent of non-certified respondents said they either "strongly" or "somewhat" agree that not having a certification restricts them to access to career advancement opportunities. Conversely, 77% of the certified information security respondents either "strongly" or "somewhat" agreed that having a certification provides them with greater access to job opportunities. In addition, about three quarters (74%) of the certified respondents believe their certifications provide them with a competitive advantage against non-certified security professionals with similar experience.

What I believe is interesting about this information is the false sense of security certifications provide. While certifications may indeed provide you with access to opportunities, they are a long way from guaranteeing you will be hired. During times when the job markets are tough, certifications are rarely the difference maker. The key in difficult employment markets is relevant experience and expertise. In my experience, many non-certified information security professionals who have developed subject matter expertise in relevant topics and have built strong professional networks have created built-in unemployment insurance that supersedes any industry certification.

It was not surprising that the main motivations of the certified respondents for achieving certifications included career acceleration, professional status and personal pride, and increased earning potential. It was also not a shock to learn the non-certified respondents did not pursue certifications due to perception of value, lack of relevance to their current job, or negative perceptions of the certification bodies. However, it did surprise me that 54% believe they have received a promotion or were selected for a job directly based on having a certification. It was not surprising that certifications played a role in this process, but what was surprising was the perception that being selected for a position or a promotion was a direct impact of achieving the certification.

CASTING CRITICAL EYE ON CERTIFICATION BODIES

When all of the certified respondents were asked if they believed that the certification bodies were primarily concerned with their members' careers, 37% either strongly or somewhat agreed, and 36% either strongly or somewhat disagreed. In addition, when asked if the certification bodies were primarily marketing organizations mostly concerned with the advancement of their organization's brand and proliferation of their proprietary certifications, 76% agreed (28% strongly, 48% somewhat) and only 8% disagreed (1% strongly, 7% somewhat). It is these numbers that generally underscore the view of information security professionals who have voiced frustration with the value of their certifications. It should serve as a wake-up call to the certification bodies that many of their constituents view them as more concerned with their business and brand, rather than the customers that they rely upon.

It should serve as a wake-up call to the certification bodies that many of their constituents view them as more concerned with their business and brand, rather than the customers that they rely upon.

Because of the CISSPs' standing in our industry and due to the fact that more than 50% of the survey respondents either hold or held the CISSP, I found these responses as some of the most interesting and telling. It was not unexpected that 62.5 percent of the CISSPs strongly or somewhat agreed that they believe that the CISSP differentiates them from those who do not possess it. What was a bit shocking was that 25% of the CISSPs stated that in order to be considered an information security professional you must be a CISSP. By utilizing this logic, in the eyes of these respondents, some of the most well noted and most successful information security leaders and chief information security officers would not be considered security professionals. There is no doubt that some would think this way, but 25% is a surprisingly high amount. What did not surprise me was that 30% of the CISSPs stated that they

would make a CISSP a requirement in hiring someone onto their team. In my experiences, many in hiring decisions like to hire people who have shared experiences and credentials. Based on this belief, I thought that this number would be a great deal higher.

From my personal perspective, it was very interesting to learn through the data about how information security professionals perceive the value of their certifications. As an executive recruiter in this industry for the past 15 years, my experiences are much different than the results. For example, very rarely have I witnessed an information security professional offered employment based exclusively on a certification or granted more compensation due to a specific certification. Conversely, on countless occasions I have heard many information security professionals claim not to be able to get through human resource and Internet key word filters without the appropriate certifications.

At the end, perception translates into reality. As an information security professional, you would be naïve to ignore market attitudes and interpretations. In the current state, there are two pieces of guidance that I can provide regarding certifications based on today's market conditions, either join 'em or beat 'em. If having a certification breaks down barriers to attain your career goal, do not let this be an obstacle and go get the necessary certification. The other choice is to make a commitment to your professional development through a combination of experience, education, talent, and brand that will make certification irrelevant.›

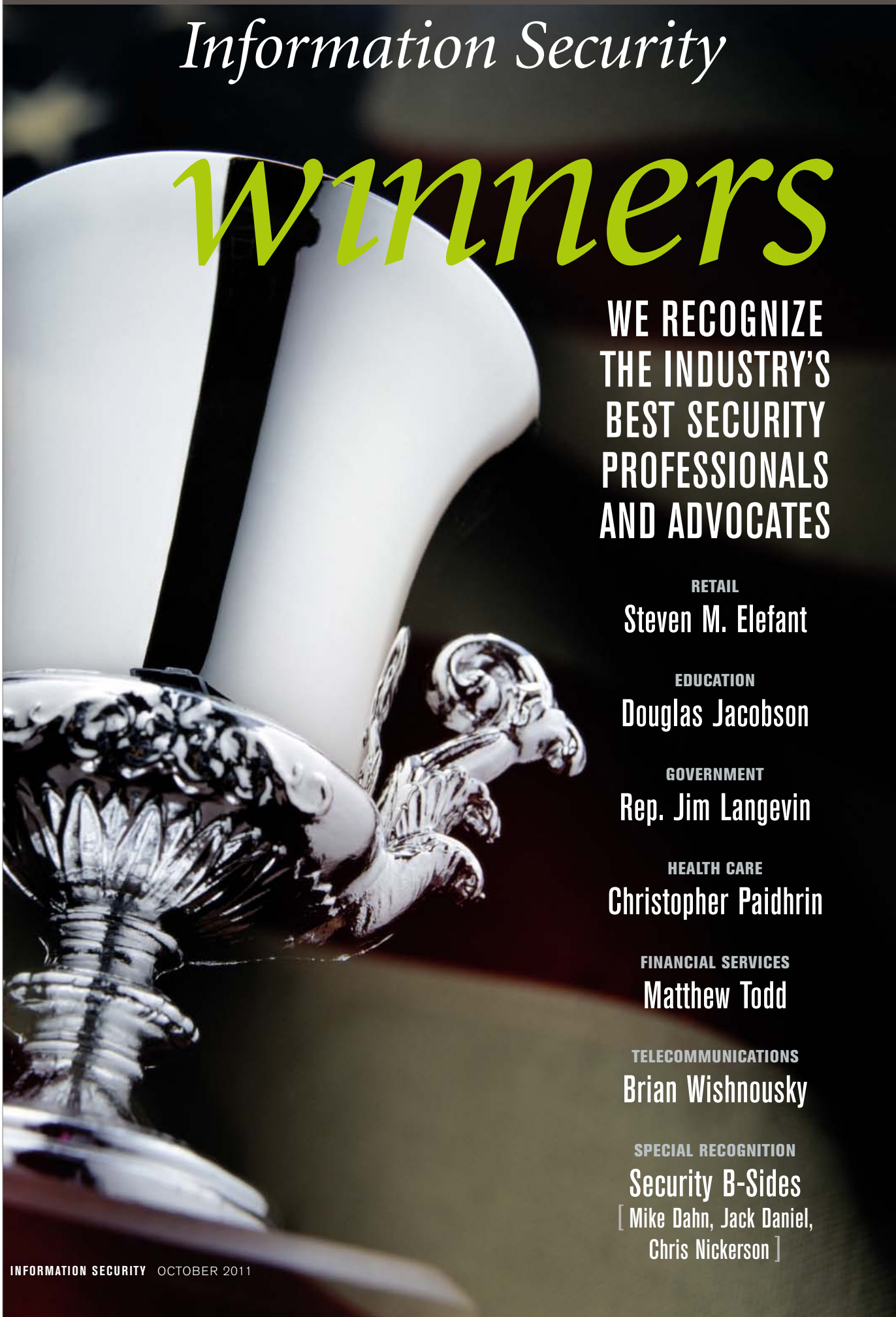
SYMANTEC IS VIRTUALIZATION.

Reap the benefits of increased flexibility with storage, security, and management software that's optimized for virtualization.

VISIT SYMANTEC.COM

Confidence in a connected world. Symantec™

Information Security winners



WE RECOGNIZE THE INDUSTRY'S BEST SECURITY PROFESSIONALS AND ADVOCATES

RETAIL
Steven M. Elefant

EDUCATION
Douglas Jacobson

GOVERNMENT
Rep. Jim Langevin

HEALTH CARE
Christopher Paidhrin

FINANCIAL SERVICES
Matthew Todd

TELECOMMUNICATIONS
Brian Wishnousky

SPECIAL RECOGNITION
Security B-Sides
[Mike Dahn, Jack Daniel, Chris Nickerson]

Secure Payments

End-to-end encryption is needed to protect the payments infrastructure. BY STEVEN M. ELEFANT

THE OLD SAYING is true: Money really does make the world go 'round. What many people don't realize is what it takes to make the money go 'round, so to speak.

When it comes to credit and debit card payments, several entities are required to process a transaction from start to finish: consumers and their payment cards, merchants and their point-of-sale (POS) payment systems, the card brands (i.e. Visa, MasterCard, Discover Network, American Express), issuing banks, and card processors like Heartland Payment Systems, the nation's fifth largest payments processor. Enormous amounts of electronic data and digital currency flow through this payment ecosystem as billions of transactions are processed each year.

With access to the sensitive information that enables the exchange of billions of dollars in transactions each year, the payments infrastructure is a red-hot target for hackers. I have been entrenched in the electronic commerce industry for more than 30 years and never before have we been at a more critical juncture in our fight against cybercrime than now. It's us good guys against the bad guys, and we are determined to win.

Forget the 14-year-old hacker kids. We are dealing with high-tech felons—the bank robbers of the 21st century. They are organized in criminal gangs, both in the U.S. and overseas, that are very sophisticated, well funded, and, in many cases, have nation-state protection.

It's no secret the payments ecosystem is vulnerable. Much like the Internet, the payments infrastructure was developed for connectivity, not for security. Now, in the face of serious threats and too many successful instances of hackers exploiting the vulnerabilities of the system, the industry is playing catch up to safeguard it.

Typically, when a consumer swipes his or her credit or debit card at a merchant location to make a purchase, cardholder data is in the clear as it leaves a merchant's terminal and is not protected until it is either tokenized in a gateway, or encrypted at rest in the processing platform's data warehouse. This is a fundamentally flawed security model that puts cardholder data at risk of being compromised should it get in the hands of cybercriminals who use methods like network or memory sniffer malware and RAM scrapers. This puts the entire payments ecosystem in jeopardy. In the case of a successful data

Steven M. Elefant

TITLE Former CIO of Heartland Payment Systems

KUDOS

Led IT strategy, product and business development for Heartland, which processes approximately 4.2 billion credit/debit card transactions annually.

Pioneered patent-pending E3 end-to-end encryption, which has been adopted by more than 13,000 merchants.

Handled breach of Heartland's payments processing in 2009, which led to development of E3.

Active in the formation of the Payments Processor Information Sharing Council, which facilitates industry collaboration against cybercrime.

Member of the U.S. Secret Service Electronic Crimes Task Force.

breach, merchants face the devastating financial and reputational repercussions of the compromise, and consumers may be forced to deal with the ramifications of credit card fraud, to name a few effects. For a secure online payment system, the transaction flow must be secured with end-to-end encryption.

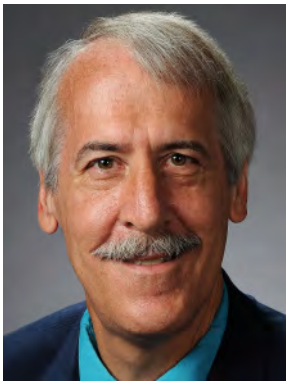
In today's day and age, there is no such thing as safe software. There never will be again. Software-based encryption is nice to have and better than no encryption at all, but has varying degrees of effectiveness. AES (Advanced Encryption Standard) is the most secure encryption available today. In fact, it is mandated by the U.S. government to protect its top-secret information. You also must consider that encrypting data after it has passed through a merchant system in the clear is quite different than encrypting data the moment a card is swiped to make a purchase. Data needs to be protected at all points, end-to-end, from the moment the transaction is initiated and through the processing network to truly be effective.

This is where hardware enters the equation. By using a hardware-protected tamper-resistant security module (TRSM), data is protected at the moment of swipe, before it enters the merchant system, beefing up security during a critical leg of the transaction lifecycle. It is this intersection of strong end-to-end encryption security software, tamper-resistant hardware and tokenization, which replaces cards' 16-digit payment account numbers with token values, that provides merchants optimal protection. By adequately protecting and removing the data that the criminals are after, we are essentially removing merchants from the hackers' crosshairs.

While technology solutions are paramount to safeguarding the payments ecosystem, industry collaboration is also an integral component in our collective fight against cybercrime. The stakes are high all around and no one can afford for threat intelligence to be a competitive differentiator. Groups like the Payments Processing Information Sharing Council (PPISC), which Heartland helped establish, have brought the industry closer in this regard, providing processors critical information and insight into cybercriminal activity. Us "good guys" need to work together so we can protect our organizations, our merchant customers, and ultimately, everyday consumers.›

Security Literacy

Tackling modern threats requires educating the general public about cybersecurity. BY DOUGLAS JACOBSON



OVER THE PAST 20 years I have witnessed the progression of computer security defenses as they reacted to the ever-increasing volume and sophistication of attacks. Emphasis on defensive approaches often focuses on purely technology-based solutions (i.e. first firewall). Today's attackers are not just exploiting software vulnerabilities, but more and more human vulnerabilities. Unlike software vulnerabilities, many of these human "bugs" cannot be simply patched with a download from the Internet; they require formal security awareness and education to mitigate. It has long been recognized there is an urgent need to improve security education and the security community needs to begin educating a broader audience than just those who work in technology.

The primary method for educating the general public about cybersecurity has been to construct "Top 10" security lists. This approach is neither effective nor sufficient as it is poor pedagogical practice to believe that students—or anyone for that matter—can remember, understand and apply knowledge when the educator provides them with nothing more than a single-page, bullet-point list of security tasks to perform. Top 10 lists communicate a false sense of security to their readers as they imply that security can be achieved simply by following these broad steps. What happens—and it will happen, often—when a student is presented with a situation not covered by a bullet point?

Formal computer security education is the key to combating the risks and vulnerabilities intrinsic to the Information Age. Each day, people are inundated with alerts and pop-ups informing them about patch updates, antivirus signatures, and firewall exceptions, but they lack the proper education or vocabulary to make value-based decisions regarding the benefits and consequences of taking specific action on these items. What a formal pedagogical approach to practical computer security education provides is the context and knowledge for students to apply computer security best practices when faced with a novel situation and the ability to be proactive, not reactive, in the face of new threats.

Computer security education shouldn't be exclusive to technical audiences. If abstracted correctly, practical security

Douglas Jacobson

TITLE Professor Electrical and Computer Engineering, Director ISU Information Assurance Center, Iowa State University

KUDOS

In 2000, led the creation of the Information Assurance Center at Iowa State University, which offers one of the largest and oldest information assurance degree programs in the country.

Oversees the Internet-Scale Event and Attack Generation Environment (ISEAGE), which is dedicated to creating a virtual Internet for research, design and testing of new cyber defense mechanisms as well as analysis of cyberattacks.

Pioneer in developing security educational programs at all levels–high school, undergraduate, and graduate.

Created computer security summer camp for high schoolers, which led to the first high school Cyber Defense Competition in 2006.

Developed a new course designed to teach basic computer security concepts to non-IT people.

education can be made accessible to readers with minimal technical backgrounds. We all perform the same basic routines on our computers and on the Internet each day. During an average day, people use passwords, connect to the Internet on an unsecure wireless connection, share media via external devices, surf the Web, click on hyperlinks, share information via social networking, and much more. Each of these actions involves a potential risk and can result in malicious consequences, many of which the average person is unaware.

At Iowa State University, we have designed a one-credit, half-semester course entitled "Introduction to Computer Security Literacy" to address this very shortcoming. The purpose of the course is to educate students of all backgrounds and IT experience levels about the inherent risks of using computers and the Internet. It is our belief that the knowledge acquired by students in this course will be immediately applicable and serve students long after they leave the university.

This course differs from past approaches as it puts security in the context of the user and benefits from the formal education setting of the university. Over the eight-week period the course is offered, students are able to internalize the information they have learned and reflect on key concepts. Students are told the real test for the course is not in the classroom, but when they leave the classroom and begin to interact with information technology—this is where the real application of knowledge occurs. They come back to class weeks later with questions that increase their understanding, have explored their computing environments in the context of security, and read, write, and talk about security on a regular basis.

Society's collective security depends on every user being security-aware and exhibiting thoughtful discipline over his or her personal information and computing resources. It has long been recognized by security experts that the user is in fact the weakest link in the security chain and technical measures alone cannot and will not solve current cybersecurity threats. So why not target the weakest link and address it in a formal educational environment?

Having presented on the topic of practical computer security to age groups ranging from elementary school children to senior citizens and everywhere in between, I can attest there is both a desire to learn and a need to provide practical computer security education to each of these respective groups (K-12, college, corporations, general public). As educators and computer security practitioners, the task of providing computer users with the opportunity to become knowledgeable about the malicious side of the Internet falls squarely upon our shoulders. Computer security literacy is not only the next step in computer security defense; it may be one of the most important steps we can take. I encourage the security profession to reach out to the public and help make it security literate.

Communication Gap

Tackling today's cyberthreats requires better information sharing between the government and private industry.

BY REP. JIM LANGEVIN (D-RI)

DESPITE THE MOUNTING risks we face in cyberspace, there remains resistance to fully addressing these problems today, as well as preventing and preparing for future threats with the most potential for widespread harm. We must improve communication between the public and private sector about threats and vulnerabilities, and institute requirements for responsible protections when necessary for national cybersecurity.

Every day intellectual property vital to our national defense and economic competitiveness is targeted and stolen in cyberspace. These threats are rapidly becoming more damaging and extensive, as highlighted through reporting from private companies that have chosen to speak up about this ongoing crisis.

A 2010 study found the average cost of a data breach for a business to be $7.2 million, but the increasing value of intellectual property makes these losses marginal in comparison to the long-term damage to America's ability to remain the world leader in innovation. A lax corporate—and often agency—attitude towards cybersecurity and the investments required to mitigate IT risks have led to a system that discourages transparency and incentivizes inaction.

As we have seen in the flood of recent news reports about targeted "hacktivism," far too often, existing products and procedures are not used by companies to protect their customers' data from the most basic threats. I support the request made by Senator Rockefeller and his colleagues who asked the Securities and Exchange Commission (SEC) to clarify corporate disclosure requirements for cybersecurity breaches. If federal securities law already requires publicly traded companies to disclose "material" risks and events, including cyber risks and network breaches, then a significant number have failed these requirements. The SEC has responded affirmatively to this push and now should follow through to ensure investor access to this information.

This is not an effort to punish those who have had an intrusion. Instead, it offers a way to provide transparency to consumers and allows the market to address this problem through customer choice.

The government, which possesses the greatest knowledge of

Rep. Jim Langevin (D-RI)

KUDOS

Co-chair of the Center for Strategic and International Studies' Commission on Cybersecurity for the 44th Presidency.

Co-founder and co-chair of the first-ever Congressional Cybersecurity Caucus.

In the 110th Congress, served as chairman of the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology; held eight hearings on cybersecurity and conducted over a dozen investigations.

Introduced the Homeland Security Network Defense and Accountability Act, which passed the House on July 30, 2008.

Introduced legislation in support of the goals of National Cybersecurity Awareness Month.

the most sophisticated cyber threats, also has a role to play. However, existing laws intended to provide important privacy protections are ambiguous about allowing the private sector to share information with the government about threats—information that would help lead to solutions. Government is similarly constrained, as the cyberthreat information it collects is most often classified and must go through a lengthy review before it can be shared with private industry.

The Department of Homeland Security (DHS) currently works with owners and operators of critical infrastructure on a voluntary basis to share information about threats to industrial control systems, but there is only a limited process for collecting threat information from public companies and many worry about legal liability or business repercussions from thorough reporting.

The Pentagon has implemented a pilot program that provides some Internet service providers with threat information to disseminate to select participating defense companies, but these efforts are currently only targeted at protecting our defense industrial base. A future model could use DHS authorities to help protect a broader customer base.

We must ramp up our efforts to provide the greatest possible threat visibility, while maintaining a strong privacy regime that prevents the government from having unnecessary access to private citizen and company data.

In the case of critical infrastructure on which we rely for public safety or national security, the risks are too serious for the government not to take some active responsibility for protecting our citizens. The threat to these entities lies in massive vulnerabilities in control systems and institutional mindsets that do not prioritize security. We already know the technology exists to cause massive damage, and we know there are numerous actors who would not hesitate to acquire it and use it against us. We cannot wait until these forces combine before we establish preventive and reactive procedures.

In some areas, such as the electric grid, the status quo is failing, while others, including the financial sector, have made substantial progress as the threat has grown. The White House's recent legislative proposals set up a useful template for dealing with these disparities by segmenting each sector under different frameworks shaped with full cooperation of that specific industry. For example, the types of threats facing smart grid technology are fundamentally different from the challenges of financial fraud. DHS should partner with sector-specific agencies and industry to institute the right mix of mandatory requirements, with penalties and incentives that make upgrading cybersecurity more cost-effective. I am looking to build off these recommendations and work with my House and Senate colleagues to move legislation forward this year.

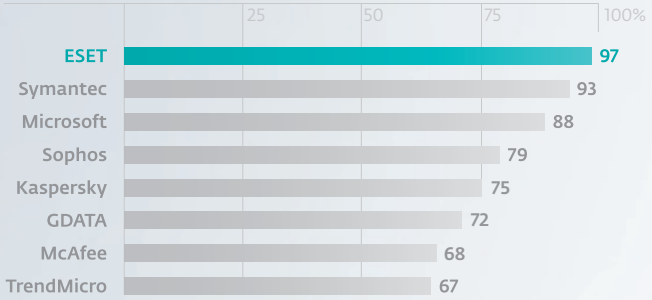
With the increased focus on cyberissues by Congress, the Administration, and our citizens, we have an opportunity to bring all the relevant parties together and establish real solutions now before this silent crisis becomes a digital disaster.›

World's No. 1

Antivirus and Internet Security

ESET leads the industry in the consecutive number of "VB100" awards from Virus Bulletin testing organization.

Virus Bulletin Awards Success ratio (%)



Selected Antivirus Vendors (not a complete list)
Source: www.virusbtn.com, May 1998 - August 2011

Limited time offer: 1 year FREE

Buy two years, get the third free

Offer valid on 25 seats or more of ESET NOD32 Antivirus Business Edition and ESET Smart Security Business Edition

10/1-12/31/11. For terms, visit www.eset.com/q4promo

eset®

www.eset.com

2011 Information Security's READERS' CHOICE AWARDS gold winner

Changing behavior

Hardwired security and privacy awareness requires a discipline of attentiveness and engagement. BY CHRISTOPHER PAIDHRIN

THE NUMBER AND severity of information breaches is rising dramatically, compounded by the expansion of social media, mobile devices, and the porous service-delivery architecture of networks. No industry or service sector is immune, including security companies. Sophisticated technologies and layers of defense cannot prevent the willful, neglectful or even unintentional actions of individuals with the capability to bypass these protections. Sadly, these individuals are often trusted staff, not only external hackers.

Numerous IT security studies have shown the significant role of unintentional behavior behind a majority of internal breaches and security incidents. These are unintended or accidental breaches, with no malicious intent on the part of individuals. The root causes are identified as lack of training, failure to follow procedure, and, increasingly, a lack of focused attention. What can be done to turn this around?

Most organizations have mandatory training, policies and procedures, and consequences for data abuse and neglect. Mature organizations also have monitoring systems, as well as compliance or awareness programs. Security best practices are followed, leadership is committed to compliance, and still, trusted team members do unwise things.

Something fundamental is missing.

The traditional goal of security awareness programs is staff compliance. Everyone is expected and required to follow policies, procedures, and organizational principles. The consequences are corrective action and possibly termination. Unfortunately, many traditional training programs fail to address the law of behavioral inertia: Behavior does not change unless it is replaced by another behavior.

Behaviors are learned, acquired and hardwired over years of practice and reinforcement; they become attributes of our persona and part of our character. Changing them is painful. Hundreds of studies have confirmed how difficult it is to change behaviors. Organizations face the added challenge of constrained resources, such as little time and funding for staff development as well as a lack of leadership skills.

Innovative organizations are trying different approaches

Christopher Paidhrin

TITLE IT Security Compliance Officer

COMPANY PeaceHealth Southwest Medical Center

KUDOS

One-person IT security team at midsize regional health care system with 3,500 employees, 90 IT professionals and 3,500 affiliated clinic workers.

Provides expert IT security, HIPAA, HITECH Act and health care technology best practices and regulatory guidance to community health care providers in southwest Washington and the Portland-metro area.

Leader for disaster recovery and business continuity planning for regional public health coalition.

Active participant in Healthcare Information and Management Systems Society (HIMSS) Security Working Group.

Created a Mind Map for IT Service Management (ITSM) to help his IT team and international audiences in understanding the complexities and interrelatedness of IT security service domains.

and techniques that address the root causes of non-compliance. When training, policies and procedures are in place, the remaining gap is "a lack of focused attention." The current business-speak equivalent is "engagement." According to research firm Gallup, engagement is more than a human resources initiative, it is a strategic foundation for the way the best organizations do business.

Author Daniel H. Pink in "DRiVE: The Surprising Truth About What Motivates Us," highlights the work of several behavioral researchers who have found that motivation in the modern workplace does not mesh with traditional "if-then" reward and punishment-based methodologies. Rather, "intrinsic" motivations like autonomy, mastery and purpose are much more healthy and rewarding for workers, and profitable for organizations. Pink's argument is that intrinsically motivated workers usually achieve more than their reward-seeking counterparts.

The customer benefits as well. Intrinsically motivated staff delivers a higher quality of service, and this has a direct correlation to customer satisfaction. For example: In the hotel sector, the research of professors Laurette Dubé and Leo Renaghan confirmed that staff "attentiveness" is the highest priority of guests.

The behavioral compliance challenge can be reduced to replacing unwanted behaviors with desired behaviors, which are "attentiveness" and "engagement." So, how does an organization foster intrinsic motivation? What do attentiveness and engagement mean in the workplace?

My definition for staff engagement would be individuals who consistently demonstrate the vision, values and mission of an organization with every action, word and gesture.

Within attention is intention. My definition for staff engagement would be individuals who consistently demonstrate the vision, values and mission of an organization with every action, word and gesture. Staff must internalize and make their own the purpose of the organization. Leadership expectations of staff compliance do not achieve behavioral change; the commitment must come from within each individual. Therefore, leadership's first priority is to strengthen the talent and capacity of intrinsically motivated employees to contribute their attentiveness and engagement to the mission. This is the missing, fundamental element of awareness programs.

Each individual's intention should manifest as a constant thought in his or her consciousness: "What is necessary now, next, and later, and what can I do to fulfill the need and exceed expectations?"

Am I giving my full attention and care to earn the trust of our customers, our patients? Do I demonstrate respect and stewardship by constantly acting with mindful, positive intention? Do I exercise precaution with hardwired attentiveness that recognizes potential harm before I take action or speak? Am I adding lasting value through my service, behaviors, and accountability to ensure good outcomes?

These then are the attitudes and behaviors all organizations would foster to ensure productive and motivated staff, and achieve service excellence. Either the workforce is actively supportive of an organization's purpose or it presents a persistent risk to its success. Either the workplace culture reinforces these desired behaviors or it doesn't.

Leaders, too, must be accountable. Leadership must refocus awareness programs to engage staff in shared ownership of the organization's mission. Leaders must be role models for the desired behaviors. Positive feedback, respect, pride of success, and joy of service for a higher purpose all strengthen a healthy workplace culture. Engaged workers thrive in environments of common vision, principles, and values.

Leaders must be role models for the desired behaviors. Positive feedback, respect, pride of success, and joy of service for a higher purpose all strengthen a healthy workplace culture.

This idea is not simply high-minded philosophy. All organizations have IT security and privacy concerns. How each organization meets the challenges of these concerns has a direct impact on both the quality of service and growth of the organization.

At PeaceHealth Southwest Medical Center, our dedicated team has been maturing our engagement efforts with what I call "Awareness In Depth." This is a layered approach to information security and privacy as well as staff engagement, which reinforces our culture of respect, stewardship, collaboration, and social justice. The principles and methodologies include:

- Multiple applicant screening criteria to assure a strong "fit."
- Rigorous interviewing processes. Select, don't hire; each team member represents the organization.
- New employee orientation.
- Confidentiality and privacy agreements, signed upon hire and each year during review.
- Policies, procedures, and processes, including appropriate use and access monitoring.
- Departmental and computer-based training; building relationships and fostering talent.
- Annual, mandatory, Web-based training modules: IT security, privacy, ethics, and appropriate use. Behaviors, even good ones, need positive reinforcement through repetition of values.
- Annual "MUMs the Word" campaign. For more than 20 years, long before HIPAA, PeaceHealth Southwest Medical Center has embraced our nationally recognized campaign of privacy and security awareness. This organization-wide annual event is a measure of commitment to a cultural behavior that we protect the information of our patients as if it were our own.
- Building trust, respect, stewardship, collaboration, and social justice.
- A culture of caring and excellence.

There is no universal agreement between theories of behavioral change, but there is broad business consensus that changes within the workplace are necessary if we are to protect information, assets, reputations, and organizational value. When behaviors are changed, each individual will be engaged and attentive, aligning him or herself with a shared purpose, as a representative of the organization, its culture, mission, vision, and values. Every customer, patient or guest should take with them a positive and memorable experience from every contact with each staff member who has earned their loyalty and trust.›

Your One Stop Shop for All Things Security

Nowhere else will you find such a highly targeted combination of resources specifically dedicated to the success of today's IT-security professional. Free.

IT security pro's turn to the TechTarget Security Media Group for the information they require to keep their corporate data, systems and assets secure. We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security standard compliance, videos, webcasts, white papers, podcasts, a selection of highly focused security newsletters and more — **all at no cost.**

Feature stories and analysis designed to meet the ever-changing need for information on security technologies and best practices.

INFORMATION SECURITY®

www.SearchSecurity.com

Breaking news, technical tips, security schools and more for enterprise IT professionals.

SearchSecurity.com

www.SearchSecurity.com

Learning materials geared towards ensuring security in high-risk financial environments.

SearchFinancialSecurity.com

www.SearchFinancialSecurity.com

UK-focused case studies and technical advice on the hottest topics in the UK Security industry.

SearchSecurity.co.UK

www.SearchSecurity.co.UK

Information Security strategies for the Midmarket IT professional.

SearchMidmarketSecurity.com

www.SearchMidmarketSecurity.com

Technical guidance AND business advice specialized for VARs, IT resellers and systems integrators.

SearchSecurityChannel.com

www.SearchSecurityChannel.com

TechTarget®
The IT Media ROI Experts

Realistic Drills

Tabletop exercises with real-world scenarios are an effective way to test your crisis planning. BY MATTHEW TODD

RECENTLY, CONSTRUCTION WORK near one of our offices resulted in a major fiber cut, taking out communications for the entire office. The call center at that office anticipated a huge call volume that week, and operations staff had a full plate of jobs to run. Thankfully, the crisis team was quickly gathered, command and control was established, response teams were called in to action, backup teams were engaged at alternate locations, and crisis was averted. Strangely enough, just a month earlier, another comparable crisis had hit the firm. Are we especially accident-prone? No—we just act that way, once a month, via a quick crisis tabletop exercise.

We've found a good tabletop exercise is an opportunity to test our "best laid schemes"—system recovery plans, business continuity plans, incident response plans, etc.—with real-world scenarios thrown in. We take a real risk, and then consider what might happen when other things go wrong at the same time, or when critical team members aren't available. We add other teams to the mix, and the teams learn from each other about risks they hadn't considered, or expertise they might share.

Planning and executing exercises has been a great way to extend my role beyond traditional information security or risk management. I have asked team leaders, executives, board members, trusted vendors and industry peers, "What keeps you up at night?" and turned the answers into something much more meaningful than another dry element in a risk matrix for consideration in the next budget cycle. When I brought players from diverse teams together, silos have shattered; IT may come with one notion of information security, but PR and legal may introduce very different ideas when it comes to leaks of material non-public information to the press or public.

Sometimes, emergency tabletop exercises serve to provide reassurance or education. A board member may be particularly concerned about an incident that occurred at a competitor. Running an exercise may help to demonstrate the processes and teams that are in place to handle just such an incident.

An exercise is an opportunity to talk to peers about what bothers them, or even about scenarios they've seen tested. One peer offered this chilling but realistic scenario: A bomb threat

Matthew Todd

TITLE CSO and Vice President, Risk and Technical Operations

COMPANY Financial Engines

KUDOS

Manages the privacy, security, availability and performance of production systems servicing over 7 million individuals.

Responsible for implementation and maintenance of systems and networks, including diverse secure data connections with eight of the largest U.S. financial services providers.

President and board member, San Francisco Bay Area InfraGard.

Worked with U.S. Department of Homeland Security on the NETGuard pilot program, an effort to help local communities respond and recover from attacks on IT systems and communications networks.

Participated in initiatives to engage SMBs in public-private partnerships such as InfraGard.

is called in to building XYZ. After playing out the response plan, which involved immediately evacuating the building to the parking lot, then came the next phase: A sniper on a building across from the main exit. There are parallels in the IT space, such as disgruntled IT staff with access to sensitive data and the skills to set a logic bomb. Sometimes a good exercise requires a suitably devious mind.

I have had the most successful exercises by keeping a few key ingredients in the mix:

Objective – Every exercise needs a clear and realistic objective, consistent with the time and teams involved. A 20-minute tabletop exercise may be fine to test the crisis management team's initial response to a media scandal or a market crisis, but would not be enough time to test the multi-team and multi-day response that might ultimately be required. If we make the objectives clear up front to all concerned, it allows the players and the coordinator(s) to identify when a topic is best set aside for another time to keep the exercise on track.

Participants – A good exercise will include one or more coordinators who present the scenario, a scribe to record the events, and the right players from across the enterprise. The coordinator(s) are prepared and have the respect of the players. The players are ready to be fully engaged in the exercise, and include individuals or managers who would be involved in the incident, even if they become "victims" along the way. Even a victim can offer observations during the exercise. When the building collapses and takes out the CFO, she may be the only one who remembers that key public filing that she needed to sign.

Realistic scene – It's critical to devise a scenario that could really happen. Alien invasions seem somewhat implausible, but just as implausible may be a scenario that exactly follows the procedure the IT team has outlined for the failure of the central email server. A more realistic scenario would be the failure of the email server at exactly the same time the entire IT staff is focused on a major virus outbreak. It may seem unfair to throw a curve ball, but reality is like that. This is the perfect time to test for resource constraints: "You say John Smith would do this next step. What if John is on vacation? Ah, Jane would take over? Well, she just came down with the flu." Consider that both virtual and real virus outbreaks can occur over the holidays.

Hotwash – Each exercise should conclude with a "hotwash," where the players and coordinator(s) gather to discuss what worked, what didn't, and what needs to happen next. Were the objectives met? What did the players learn? Are there gaps in process, procedure, people, systems or communications?

So how do I know my exercise program is successful? There are a number of strong indicators. I have had the opportunity to engage with key partners in exercise plans, and help them consider risks in a more realistic fashion. The board has taken a keen interest in the program and its results. The CEO has incorporated a mini-tabletop exercise as a regular event for his senior staff. But ultimately, exercises have resulted in meaningful dialogue and action, and participants have gained confidence and skill in how to respond to real-world adversity.›

Unexpected Benefits

A network scanning program unearths more than vulnerabilities. BY BRIAN WISHNOUSKY

WHEN WE STARTED establishing our Threat and Vulnerability Management (TVM) Program in 2010, we knew where we were heading. Although driven primarily to satisfy a regulatory requirement—PCI DSS—this was something we had been talking about for a long time as a good security practice. Scanning 80,000 IP addresses across a flat network was a big undertaking. While we knew we would be getting reams of data back from the scans, we underestimated the compelling story the data would tell.

The first year saw the program mature from a set of scans with output to a program defined by processes, specifications and reporting, not just for existing devices, but also for the new devices that are part of normal growth. An application here, a couple firewalls there, all requiring a scan before being implemented into production to ensure they're deployed in a secure manner. Now in the second year of the program, we are starting to perform further analysis on the data we're getting back from our scans. It's a lot of data, but we are starting to pull out nuggets we hadn't expected when we created the vulnerability management program.

One of the most important parts of any security program is patching. Most organizations spend a lot of effort ensuring the server infrastructure is patched in a timely manner. Desktop OS patches also get a lot of attention, as do the most common desktop applications. What doesn't get a lot of attention, from a patching perspective, are all the other applications that make up your business users' requirements (e.g. Adobe products, Java, developer tools, productivity tools) that may or may not be centrally supported. The TVM Program is starting to fill this gap. The scan reports tell us not only about OS problems, but also about problems with installed applications on the desktop/server infrastructure. These reports, when presented, not only get all the ancillary applications patched, but also assist in getting the complete application picture included in the overall patch management processes. We now have a full view of the additional software users put on their machines, which gives us a clearer picture of the threat profile of the systems on the network.

As part of the TVM Program, we do a monthly mapping exercise to keep track of what we are scanning. It's amazing to see the numbers change month to month. It's also interesting

Brian Wishnousky

TITLE Senior Manager, Threat and Vulnerability Management

COMPANY Rogers Communications

KUDOS

Led the creation of the Threat and Vulnerability Management program at Rogers Communications. He is responsible for the TVM Program, which encompasses roughly 75,000 internal IP addresses, and 2,000 external IP addresses.

Instrumental in the creation of security standards and policies at Rogers, contributing to a vastly improved security posture for the corporate network.

Leads the security vendor management process for the Information Security Office at Rogers.

to compare the number of devices on the network with the number of "supported" devices that are in our company's asset database. When we started the program, we knew we would be contributing to the asset database, simply because we would be getting a very clear picture of what should be there. What we did not expect was having a large number of "rogue" systems for which we could find no owner and, in some cases, no one acknowledging the existence of that device.

Some of these unknowns are consumer devices (iPhones, iPads, Androids and BlackBerries), but some are business computing devices (servers/workstations) or network devices (switches, home routers with WiFi) that people put on the network to "make their jobs easier." It's nice to see people trying to be more efficient, but it makes our job more difficult. A lot of these rogue devices are not properly patched, do not have basic security software, and are not properly hardened against attacks, which could turn them into launch-pads for malicious attacks. We can't change the way people think overnight, but by having the data reported on regularly with the scans, the risk posed by these devices can now be rated, and dealt with as appropriate. It's one thing to know you have these devices, but quite another to see them and to have the risk identified and quantified.

Another beneficial off-shoot of the TVM Program is identifying problems with the asset database. While every attempt is made to keep the database updated, things get missed, updates don't happen due to job changes and often, errors are made. The TVM Program cannot fix these errors, but again, it does a good job of identifying errors in the data—such as incorrect IP address, location or owner information—and in some instances, can provide updated information for the database. This is a harder problem than it appears, because the TVM Program depends on the asset database for a lot of the information regarding whom to send reports. Without that owner information, scanning, patching and asset lifecycle management will eventually come to a screeching halt, so we try to be proactive in making sure the database is updated properly.

I am sure as we move into the third year of the program and beyond, we will find more ways of using the new information we are creating and will reap additional benefits from our TVM Program.›

B-Sides Themselves

Security B-Sides conferences break the mold of traditional security events, fostering participation and collaboration among professionals. BY MIKE DAHN, JACK DANIEL AND CHRIS NICKERSON

THE B-SIDE OF a record was always our favorite. They were the artist's edgy, artistic and passionate songs—the songs that may not appeal to the masses or be in vogue, but truly showed the artists in their natural light. The A-side was for record producers and mass media, but the B-side was where the real band lived. That is exactly how we feel about Security B-Sides conferences.


Mike Dahn


Jack Daniel


Chris Nickerson

The events, locations and talks are not just about what's hip. B-Sides conveys the art and passion of the participants who don't always get airplay via mass media channels. B-Sides talks are a conversation between the speaker and the audience to get a fully engaged experience. B-Siders have removed the barriers to entry and castes that exist in the conference setting, and replaced them with communication, collaboration, innovation, and choice.

This choice is the heart of each event. While mainstream conferences have a templated method of delivery, each B-Sides event is unique as evidenced by the "Don't Mess with Security" theme in Texas to "Berlin Sides" in Germany. Each event is customized to the local people who participate in putting it together. B-Sides enables this choice while maintaining common goals and values, including:

- **Each event is 100 percent free to all participants.** This enables a diverse audience of ideas and communication. When people ask what the demographics of a B-Sides event are, we do not talk about career titles. Instead, we say the one thing participants have in common is to engage and discuss. If speakers come with a great idea, that will be amplified. If speakers come with a bad idea, that will be amplified.
- **Events are positive collaborations – the goal is to elevate, not denigrate.** These events follow the mantra: "Do no harm." Though few are trying to boil the ocean, we see these events as another

Security B-Sides

KUDOS

- Founded in 2009 by Mike Dahn, Jack Daniel and Chris Nickerson.
- First event: B-Sides Las Vegas, July 29-30, 2009.
- 40 events worldwide to date.
- Events have been held on six continents.
- B-Sides provides a framework for security professionals to organize and build community events. Attendees are considered participants and encouraged to collaborate with session presenters and network with other participants.

way of connecting people and ideas to help raise the bar and elevate the conversation. We can all see further when standing on the shoulders of giants.

- **We love our benefactors, but there are no vendor booths or expos.** Sponsors participate just like everyone else. Some provide capital; others bring the beach towels. We tell our sponsors the same message we tell everyone, that the best way to obtain value from a B-Sides event is to have your people participate.

B-Sides events are more a community gathering than just a conference. It is the quintessential "commons" where people can connect and collaborate on ideas, on stage, in the kitchen or around the pool. Participants attend to build relationships. These relationships enable a natural flow of information beyond just the one-hour speaker time block.

If a rising tide raises all ships, then this "commons" enables the flow of information and relationships that help raise the level of conversation within the security community. We share many of the same goals, but have experienced very different ways of achieving them. The more ideas we have, the better the solution becomes.

Creating a free and open commons requires pushing the expectations of everyone involved. Instead of hosts and attendees, everyone at a B-Sides event is a participant. The audience and speaker participate in a conversation. Volunteers, organizers and sponsors participate and build upon each other's resources and experiences. The success of such a commons is based on the participation of everyone involved. Similarly, security should not be the role of one department in an organization, but rather a collaboration between everyone within an organization. Security can only be its best when everyone is a participant in the process.

People attend events for the community and leave wanting to further connect their own local community. As B-Sides conferences grow, we see participants customize and localize their event. Some are rowdy while others are tame. Some are more formal, while others are in a pool somewhere in the desert. There is no universal template or guide book to security. It takes the customized participation of everyone involved. There are no innocent bystanders or collateral damage in security. Everyone within an organization is affected and as such they should all be involved in the solution.

From boat to boardroom, B-Sides enables community participation that raises the bar of security in the industry and the organizations those people represent.›

honor roll

2010

Phil Agcaoili
Brian Engle
Blanca Guerrero
Christopher Ipsen
Nick Mankovich
Julie Myers
Ezzie Schaff

2009

Jerry Freese
Melissa Hathaway
Bruce Jones
Jon Moore
Adrian Perrig
Bernie Rominski
Tony Spinelli

2008

Bill Boni
Mark Burnette
Michael Mucha
Marc S. Sokol
Gene Spafford
Martin Valloud
Mark Weatherford

2007

Michael Assante
Kirk Bailey
Michael Daly
Sasan Hamidi
Tim McKnight
Mark Olson
Simon Riggs

2006

Stephen Bonner
Larry Brock
Dorothy Denning
Robert Garigue
Andre Gold
Philip Heneghan
Craig Shumard

2005

Edward Amoroso
Hans-Ottmar Beckmann
Dave Dittrich
Patrick Heim
Christofer Hoff
Richard Jackson
Charles McGann

STOP ADVANCED ATTACKS IN THEIR TRACKS

Another day, another breach. And it's not just the big guys losing data anymore. Cybercriminals are now using advanced attacks to steal data from companies of every size. How? They exploit the gaps in your traditional defenses to infect your systems with malware and exfiltrate your valuable data. Websense® TRITON™ security helps protect against threats coming in through the web and email, and helps stop data from leaving when it shouldn't.

- **Anatomy of APTs and other advanced attacks**
- **How common cybercriminals used advanced attacks to steal data**
- **Solutions for defending yourself**

Learn more in this webcast

Today's productivity tools are increasingly mobile, social, and in the cloud. But so are advanced data-stealing attacks, which antivirus and firewall can't prevent. You can stay a step ahead with Websense® TRITON™ security, which combines best-of-breed web security, email security, and DLP modules (available together or separately) into one powerful solution. With shared analytics, flexible deployment options, and a unified management console, it's the effective and economical solution for today's security challenges.

websense®

NOT YOUR MOTHER'S ANTIVIRUS

TRADITIONAL ANTIVIRUS TOOLS HAVE MATURED INTO MULTI-FEATURED ANTIMALWARE SUITES. HERE'S WHAT YOU SHOULD KNOW WHEN SHOPPING FOR ENDPOINT PROTECTION.

BY LENNY ZELTSER

Protecting endpoint computers from malware is critical to providing reliable operations, safeguarding data and maintaining an acceptable compliance posture. Standalone antivirus products of the past have matured to encompass a variety of tools for securing endpoints in an enterprise setting. As the threats associated with malicious software increase in sophistication, so do the capabilities of antimalware tools. Understanding the capabilities and limitations of components that form an enterprise antimalware suite is critical to selecting the right product for your organization and deriving value from it.

One way to understand what components we can expect to find in an antimalware product suite is to consider how malicious software often propagates:

- Through the victim's browser
- Via email in the form of malicious links and attachments
- Through local network and removable media
- Via exploits and social engineering tricks

An antimalware product suite should tackle all these infection vectors, attempting to stop malware before it begins running on the protected computer. For these reasons, anti-malware products typically incorporate components for safeguarding browser activities, overseeing email attachments and spam, controlling the system's network activities, and blocking various types of exploit attempts.

The strength of an antimalware suite is not only in the solid implementation of these individual features, but also in the extent to which the multiple components are integrated with each other to offer reliable protection, even if a single measure fails. Moreover, they must accomplish this in a way that scales for many systems in an enterprise setting. Let's take a closer look at the capabilities of antimalware product suites to understand what they involve and what limitations they might possess.

CORE ANTIVIRUS FUNCTIONALITY

Traditional antivirus techniques form the cornerstone of many antimalware suites. On-access or real-time antivirus protection involves blocking the execution of malicious code before it has an opportunity to cause significant damage. Antivirus tools also allow the user or system administrator to launch on-demand scans, which will scan the file system, removable media, memory contents and network shares. Similarly, scans can be scheduled to occur with the desired frequency automatically.

Identifying malware the vendor has seen earlier can be done with high efficiency by using static signatures, such as sequences of bytes or hashes of files. The bigger challenge involves detecting new malware, for which the vendor has not yet developed a signature. Most antivirus tools accomplish this by relying on heuristics and behavioral patterns, which indicate a program possesses malicious characteristics.

In addition to identifying and blocking malware, antivirus tools can also automatically remove some malicious software from the infected computer. However, enterprises should be cautious when relying on such capabilities. If the malicious program had the opportunity to run on the system before being removed, it's possible additional malware components were installed there without being detected by the antivirus tool. Similarly, the attacker may have used the malicious program to remotely access the system to install additional tools or cause other damage. A more reliable method is to reimage the infected computer rather than attempting to disinfect it.

In addition to the traditional antivirus mechanisms outlined above, products designed to protect computers from malware incorporate additional defensive capabilities; which components are incorporated into the baseline antivirus offering and which are available as part of a larger antimalware suite depends on the vendor.

SPYWARE AND ROOTKIT PROTECTION

Many malicious programs incorporate some form of spyware capabilities, be it capturing the victim's keystrokes, recording mouse interactions, capturing screenshots, intercepting browser form submissions, recording webcam and microphone signals, or stealing documents. Similarly, malware may have rootkit characteristics that allow it to hide from many system administration and security tools, complicating the task of detecting and analyzing the security incident.

Because spyware and rootkit capabilities of malware form a significant threat, the makers of antispyware suites often incorporate and highlight features explicitly designed for curtailing this attack vector.

Because spyware and rootkit capabilities of malware form a significant threat, the makers of antispyware suites often incorporate and highlight features explicitly designed for curtailing this attack vector. This way, even if the malicious programs aren't blocked by other components of the suite, their effect on the protected system may be dampened: The product may be able to notice and block attempts by spyware to capture data. It may also identify inconsistencies in the way the system behaves to spot the presence of a rootkit and disable it.

HOST FIREWALL AND INTRUSION PREVENTION

Antimalware suites typically include a component that replaces the host firewall included with the operating system. This usually provides a more full-featured way of controlling traffic to and from the protected system. For instance, the firewall can learn which programs are expected to send Internet-bound traffic over certain ports, and block other outbound network activities.

The more mature the product, the more capabilities its firewall will have to automatically make decisions according to the vendor's understanding of common software and the policy defined by the enterprise administrator. In fact, one of the advantages of replacing the firewall built into the OS is the ability to control network security settings of the computer by using the centralized console that is part of the antimalware suite.

RSA® CONFERENCE 2012

FEBRUARY 27-MARCH 2 | MOSCONE CENTER | SAN FRANCISCO

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

SAVE $700

Before Friday, November 18, 2011

For more than 20 years RSA® Conference has been a roundtable for information security experts, thought leaders and practitioners from around the globe. Amidst an onslaught of security threats and attacks, we invite you to RSA® Conference 2012 to experience the power of our community.

Come arm yourself with the tools, network and insights needed to protect your kingdom.

MULTIPLY YOUR INSIGHTS
Over 220 expert-led sessions.

BROADEN YOUR PERSPECTIVE
Attend world-class keynotes.

STRENGTHEN YOUR SOLUTIONS
Discover innovative products and services.

BUILD YOUR NETWORK
Connect and share with information security's best and brightest.

REGISTER NOW!

www.rsaconference.com/techtarget

Antimalware suites also include a host intrusion prevention component, designed to block exploits. A mature intrusion prevention module will be able to block exploits by not only matching the signature of known exploit code, but also by identifying variations of the exploit pattern. This is yet another defensive layer, designed to protect the system if other aspects of the antimalware suite fail.

Host intrusion prevention modules pay particular attention to client-side exploits by integrating into the system's network stack and, sometimes, by installing a browser add-on. This allows the tool to offer protection even if the user connects to a host that wasn't known to be malicious at the time, and is especially important for handling threats associated with client-side exploits. The intrusion prevention module can also oversee local processes, which is especially helpful when a program that found its way onto the system is exploiting a local vulnerability for privilege escalation. When designing the intrusion prevention module, an antimalware vendor needs to carefully balance the tool's ability to block malicious actions with the likelihood that it may inadvertently prevent legitimate operations.

SECURING THE WEB BROWSER

Considering the high number of infections that involve the Web browser in at least some form, it's important for an antimalware suite to wrap a security blanket around the user's browser. Two attack strategies are worth considering when examining the tool's ability to protect the browser:

- A remote website may attempt to exploit a vulnerability in software installed on the computer. This can occur when the victim visits the website directly, is referred to it by another site such as a search engine, or observes a banner ad that contains malicious code.
- A remote website may attempt to persuade the visitor into running a malicious program without exploiting a vulnerability in software. A common social engineering trick to accomplish this involves convincing the person to install a fake antivirus tool that is actually malware.

Some aspects of these threats can be tackled using other components of an antimalware suite, including traditional antivirus protection and intrusion prevention capabilities. However, it's worth it to first try stopping the attack closer to the source—within the browser itself. To accomplish this, the browser security component of the suite often includes the following capabilities:

- Blocking attempts to access websites that are known to be malicious. To accomplish this, antimalware vendors track reputational details for websites, maintaining frequently updated lists of known good and bad sites.
- Examining the code executed by the browser—most notably JavaScript—to identify malicious scripts based on signatures, heuristics or behavioral patterns. However, accomplishing this in a way that doesn't rely heavily on signatures, yet doesn't slow down the user's experience, isn't easy.

• Scrubbing search engine results. The tool may insert information into the search results page to inform the user about the reputation of websites before he or she attempts to visit them.

EMAIL SAFEGUARDS

We're increasingly using Web browsers for electronic communications, be it interacting with social networking sites, using webmail or sharing files. Yet, traditional email tools continue to play a pivotal role in enterprises. As the result, antimalware suites typically incorporate components for safeguarding this communication channel.

Spam filtering is a common component of antimalware suites. The need for blocking spam has been apparent to enterprises for many years. As a result, spam protection tends to be a very mature part of many antimalware suites.

Addressing email as a potential attack vector also involves flagging received messages that resemble phishing attempts, disabling links to potentially dangerous sites and scrutinizing attachments. The tool may disable attachments that don't match the file types approved by the administrator. It also scans the attached file with the antivirus component of the suite. In addition to examining inbound emails, the email security module may also monitor the messages sent by the protected system: Outbound messages that have malicious attachments and those sent too rapidly would be blocked and used as an indicator that the system is infected.

Addressing email as a potential attack vector also involves flagging received messages that resemble phishing attempts, disabling links to potentially dangerous sites and scrutinizing attachments.

CLOUD-BASED ASPECTS

The vendors of antimalware suites are increasingly incorporating community-oriented capabilities into their products, finding ways of collecting and analyzing data from some systems to benefit the rest of the user population. Such functionality is sometimes marketed under the moniker of cloud-based antivirus capabilities.

Instead of relying purely on local processing to determine whether a file is malicious, an antimalware tool with cloud capabilities captures the relevant details from the endpoint and provides them to the vendor's centralized infrastructure for real-time processing. The vendor examines the data, potentially correlating it with information obtained from other systems, and issues a verdict regarding the risk level of the file to the endpoint. This approach helps

the antimalware product identify malware even if the file was not known to be malicious a few instances earlier.

A significant component of many vendors' implementations of community or cloud-based capabilities is the reputation of files. For instance, when a system encounters a new executable, it can query the vendor's "cloud" to determine the file's popularity among other members of the community. An executable that is unique to a system is likely to be malicious or, at least, is suspicious. Antimalware products may incorporate similar reputational capabilities with respect to URLs and email messages for the benefit of other components of the suite.

CENTRALIZED MANAGEMENT CAPABILITIES

Organizations need to be able to control hundreds, even thousands of systems running the antimalware suite. To support this requirement, vendors generally include a centralized management console as part of their products. This is a critical capability, since handling the installation, oversight and troubleshooting of individual instances of the product doesn't scale in the enterprise setting. With this in mind, enterprise-focused antimalware suites generally allow administrators to perform the following remote functions from a centralized console:

- Install, upgrade and configure antimalware products on endpoints.
- Collect and review alerts related to the product's functionality and malware events.
- Manage false positives related to erroneously blocked files, URLs, email messages, etc.
- Run scheduled or ad-hoc scans on some or all systems in the organization.
- Identify "rogue" systems that should, but do not have the product installed or enabled.
- Generate reports for reviewing the metrics related to the organization's antimalware posture.
- Deploy emergency signatures or other updates when handling a malware outbreak.

The way in which an antimalware product will be managed needs to be compatible with other security-related tools and processes within the organization. That's why antimalware vendors often include the ability to integrate their centralized management consoles with Active Directory and log management tools.

DEPLOYMENT CONSIDERATIONS

Considering most antimalware suites incorporate the features outlined above, one product might be a better choice for one enterprise than another based on factors such as:

- How effective they are at identifying and blocking malicious actions: Independent labs periodically evaluate the capabilities of antimalware tools. Review reports from several sources, while paying attention to the components and use cases that have been tested.

- How intrusive they are on users' day-to-day activities: Some antimalware tools place a heavier load on the system than others. Moreover, the tools differ in the extent to which their user interface elements overwhelm users with questions or other annoyances.
- What capabilities they provide to administrators for handling malware outbreaks: Consider what features—such as logging, remote installation, emergency signature deployment, and quarantine management—will be valuable to help you analyze and contain a security incident that involved malware.
- Where their components can be installed. While the focus of this article has been workstation protection, antimalware tools often include components that can be installed on servers, mobile devices and network boundaries.

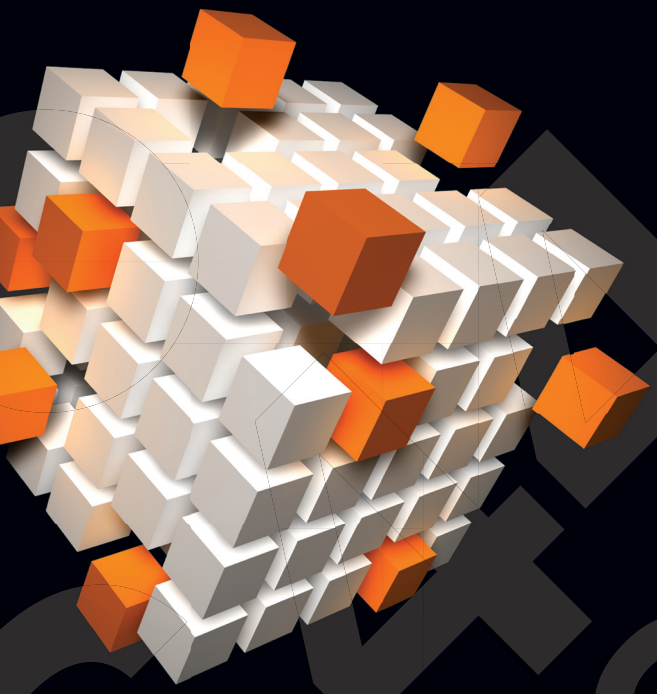
Antimalware suites incorporate several components for protecting a system from malware because a single layer of defense is more likely to fail than several tools integrated together. Similarly, an antimalware suite running on the endpoint is only a single defensive measure in the context of the enterprise at large. As you explore the capabilities of the antimalware suite that you already own or are planning to purchase, consider how it fits into the overall enterprise security architecture.›

Lenny Zeltser is a seasoned information security professional with a strong background in online threats and defenses. He teaches malware combat courses at SANS Institute. Send comments on this article to feedback@infosecuritymag.com.

Source 44 Consulting

www.source44.net

Network and Data Security Services



Threat Mitigation

Network & Security Technologies

Security Assessments

Network Audit / Security Architecture Review
Vulnerability Assessments
Penetration Tests
Incident Response
Forensic Readiness Assessments

Support Services

Professional Services & Full Support
Security Infrastructure Management

Digital Forensics

Investigations
Data Recovery
e-Discovery
Litigation Support

IT Security Training

Training Courses

Contact us for a **FREE**

1-hour consultation

info@source44.net

905.237.4576

For your SPECIAL OFFER please scan the QR Code

www.source44.net

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY®

EDITORIAL DIRECTOR
Michael S. Mimoso

SENIOR SITE EDITOR Eric Parizo

EDITOR Marcia Savage

SENIOR MANAGING EDITOR Kara Gattine

NEWS DIRECTOR Robert Westervelt

SITE EDITOR Jane McPherson

ASSOCIATE EDITOR Carolyn Gibney

ASSISTANT EDITOR Maggie Sullivan

UK BUREAU CHIEF Ron Condon

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS
Marcus Ranum,
Lee Kushner, Mike Murray

CONTRIBUTING EDITORS
Michael Cobb, Philip Cox,
Scott Crawford, Peter Giannoulis,
Ernest N. "Ernie" Hayden,
Robbie Higgins, Jennifer Jabbusch,
David Jacobs, Diana Kelley, Nick Lewis,
Richard E. Mackey Jr., Kevin McDonald,
Sandra Kay Miller, Ed Moyle, Lisa Phifer,
Ashley Podhradsky, Ben Rothke,
Anand Sastry, Dave Shackleford,
Joel Snyder, Lenny Zeltser

USER ADVISORY BOARD
Phil Agcaoili, Cox Communications
Richard Bejtlich, GE
Seth Bromberger,
Energy Sector Consortium
Chris Ipsen, State of Nevada
Diana Kelley, Security Curve
Nick Lewis, Saint Louis University
Rich Mogull, Securosis
Craig Shumard, CIGNA CISO Retired
Marc Sokol, Guardian Life
Gene Spafford, Purdue University
Tony Spinelli, Equifax

INFORMATION SECURITY DECISIONS
GENERAL MANAGER OF EVENTS
Amy Cleary

VICE PRESIDENT/GROUP PUBLISHER
Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Kathleen Quinn

SALES DIRECTOR Tom Click

CIRCULATION MANAGER Kate Sullivan

PROJECT MANAGER Bryce Dooley

PRODUCT MANAGEMENT & MARKETING
Kim Dugdale, Andrew McHugh,
Karina Rousseau

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Patrick Eichmann
peichmann@techtarget.com

Sean Flynn seflynn@techtarget.com

Jennifer Gebbie
jgebbie@techtarget.com

Jaime Glynn jglynn@techtarget.com

Leah Paikin lpaikin@techtarget.com

Jeff Tonello jtonello@techtarget.com

Vanessa Tonello
vtonello@techtarget.com

George Whetstone
gwhetstone@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER
Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT
Kevin Beam

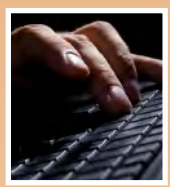
CHIEF FINANCIAL OFFICER
Jeff Wakely

EUROPEAN DISTRIBUTION
Parkway Gordon
Phone 44-1491-875-386
www.parkway.co.uk

LIST RENTAL SERVICES
Julie Brown
Phone 781-657-1336 Fax 781-657-1100

COMING IN NOVEMBER





Virtual Desktop Infrastructure

VDI is an emerging technology that provides the opportunity to re-architect endpoint security and management. VDI allows your organization to centrally control desktop images and configurations to lessen the risk of non-compliance with security policy. It also reduces licensing costs and additional costs associated with malware and the loss of regulated data. In this feature, you'll learn about VDI security options, how to evaluate what products best fit your environment and what the ideal configuration looks like.

Cybercrime

The threat landscape is changing—again. Organized criminals operating on the Internet are targeting smaller organizations with fewer security resources and tools in place. This article will look at the shifting landscape, including an in-depth look at the tactics and tools hackers are using to steal private data and the shift in focus away from credit card data to intellectual property.

Risk Assessment

Information risk assessments can and should be valuable processes but too often the risk assessment process is used to get a desired outcome. An effective risk assessment program should drive an organization security initiatives and its program. It should not be a process to show compliance to regulations or adherence to good security practice.

Don't miss our monthly columns and commentary.

TechTarget
Where Serious Technology Buyers Decide

INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 275 Grove Street, Newton, MA 02466 U.S.A.; Toll-Free 888-274-4111; Phone 617-431-9200; Fax 617-431-9201.

what drives *your* approach to IT security?

Balancing business priorities and risks is key to a solid approach.

SystemExperts helps you build a comprehensive and cost-effective information security plan that makes sense for your company. Right now, our **ISO 17799/27002 Compliance Program** helps you to focus resources on your most important business risks and comply with regulations such as **Sarbanes-Oxley, FFIEC, HIPAA, PCI,** and **Gramm-Leach-Bliley.** Best of all, our approach works equally well for "Main Street" businesses and the Fortune 500 clients we've proudly served for years.

If you want a practical IT security plan that addresses your real business risks, contact us today at 888.749.9800 or visit our web site at www.systemexperts.com/public.

- ISO 17799/27002 Compliance
- HIPAA and PCI DSS Compliance
- Application Vulnerability Testing
- Security Audits and Assessments
- Security Architecture and Design
- Identity Management
- Penetration Testing
- Security Best Practices and Policy
- Emergency Incident Response
- System Hardening
- Technology Strategy
- ASP Assessments

SystemEXPERTS
LEADERSHIP IN SECURITY & COMPLIANCE

See ad page 10

- Read the results from the Ponemon Institute's Second Annual Cost of Cyber Crime Study
- Critical Capabilities for Security Information and Event Management Technology - Gartner 2011

See ad page 7

- Data Loss Prevention in the Network and Beyond
- Deny Data Loss

See ad page 14

- Finally! Audit UNIX, Linux and Windows Server Activity. View the Centrify DirectAudit Demo
- Centrify DirectAudit - Audit Any Server Activity. Download the whitepaper.

See ad page 27

See ad page 4

- First Half 2011 Security Labs Report
- Simplifying Email Compliance, Policy, and Management

See ad page 19

- Securing the Cloud for the Enterprise
- Cloud and Midmarket Success Criteria

RSA CONFERENCE 2012
FEBRUARY 27 – MARCH 2 | MOSCONE CENTER | SAN FRANCISCO

See ad page 44

- Follow the latest webcasts and blogs from your community of top security professionals
- Register for RSA Conference 2012 before November 18,2011 to recieve Early Bird Savings of $700

websense®

See ad page 40

- Arm yourself against APTs
- Websense Advanced Classification Engine