

SecurityAgenda

Information Security and Risk Management News & Insights

February 2012

The Year of **MOBILE SECURITY**

BYOD: How to Minimize Risk

The question isn't whether your employees will use their mobile devices. It's how you'll secure them. **p.16**

FEATURING

How to Enforce Your Mobile Policy

p.21

Malcolm Harkins: Intel's CISO on How to Manage the Risks of Mobility

p.22

PLUS

Top 10 Breaches of 2011: What We Learned

Careers: Growing the Team



2012 GOALS

~~2 X~~ Keep Boss Happy!
(Prepare for next year's compliance audit)

~~1? X~~ Keep Spouse Happy!!
(Travel less for work...)

3. Advance my Career
(Brief the Board...on this year's
Privacy & Risk Management Programs)

Meet all your goals this year...

...with online education from BankInfoSecurity.com.



Information Security | Risk Management | Compliance | Fraud

100% Online | 24/7 Access | 130+ Courses

www.bankinfosecurity.com/memberships



16 Mobile Security

Cover Story: 2012: The Year of Mobile

16 BYOD: How to Minimize Risk

Increasingly, organizations are surrendering to armies of employees who want to use their personal mobile devices to conduct business. How can a security leader proactively protect the organization, individuals and devices from mobile computing risks?

21 How to Enforce Your Mobile Policy

A mobile computing policy is like an Internet usage policy – every organization has one. But how well is it enforced? Here are expert insights to ensure you put your policy into practice.

22 BYOD: “It’s Going to Happen”

Interview with Malcolm Harkins, CISO of Intel, on how his organization has managed what’s going to be one of the top challenges of 2012.

Also Inside:

8 Careers: Growing the Team

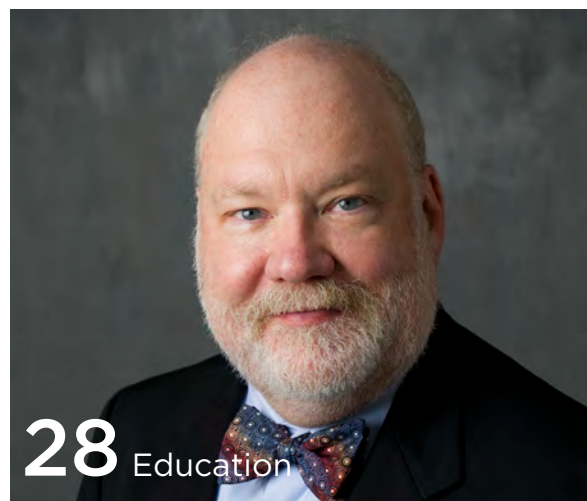
There are jobs aplenty for today’s information security professional, but how does a security leader go about filling these open positions with the right staff? Security and hiring leaders offer tips.

10 A Wake-Up Call for Risk Management

The slew of data breaches over the past year has raised the consciousness among businesses and governments of the need to manage risk more than ever before.

24 Roadmap to Securing Online Transactions

The FFIEC Authentication Guidance is aimed specifically at U.S. financial institutions, but the recommended processes and controls are applicable to most global entities. See how.



28 Education

Interviews:

6 ENISA Tackles Cybersecurity

The European Network and Information Security Agency on its efforts to improve information security awareness across Europe.

26 Automation with a Dash of Humanity

Roundtable discussion: NIST’s Ron Ross and other information risk leaders offer expert opinions on the key agenda items for 2012.

28 The State of Security Education

Purdue’s Eugene Spafford on information security education and why today’s aspiring pros have to work harder to prepare for their careers.



10 Breach Response

Meeting the Mobile Challenge

BYOD – you can't go anywhere without hearing the acronym these days.



Tom Field

The bring-your-own-device phenomenon has swept global businesses, and the challenge only intensifies with every new wave of smart phones, tablets and portable storage devices. It's no longer a question of whether organizations will allow employees to use their own mobile devices. That's already happening. The real question is: How will you secure their usage?

Mobile security is the cover story of this 2012 edition of Information Security Media Group's Security Agenda – our annual overview of the year's top priorities. Included in this feature package are:

- **BYOD: How to Minimize Risk**
- **How to Enforce Your Mobile Policy**
- **Intel's CISO on Managing the Risks of Mobility**

Beyond mobility, we also present a variety of features on other key topics facing security and risk management leaders in 2012. Among them:

- **Data Breaches** – See what we (should have) learned from 2011's top breaches;
- **Careers** – Roles are changing; how do you groom your team to meet the new demands?
- **Compliance** – What can other industries borrow from U.S. banking regulators' authentication guidance?

You'll find excerpts of exclusive interviews with renowned thought-leaders such as Prof. Udo Helmbrecht of ENISA and Prof. Eugene Spafford of Purdue University.

These features are a sampler of the content provided daily by Information Security Media Group, and they represent each of our growing suite of global media sites: BankInfoSecurity, CUInfoSecurity, GovInfoSecurity, HealthcareInfoSecurity – and our newest sites, CareersInfoSecurity, DataBreachToday and InfoRiskToday. Please check out all our new sites and share your feedback with me.

Meanwhile, don't miss our two RSA Conference presentations:

- **How to Launch a Secure Cloud Initiative: NASA's Jet Propulsion Laboratory**
Featuring Executive Editor Eric Chabrow and Tomas Soderstrom of NASA JPL
Wednesday, February 29, 10:40 AM, Room 305;
- **The Faces of Fraud: An Inside Look at the Fraudsters and Their Schemes**
Featuring me and Erik Rasmussen of the U.S. Secret Service
Friday, March 2, 9:00 AM, Room 102.

Best,

Tom Field,
Editorial Director
Information Security Media Group

SecurityAgenda

Editorial

Tom Field, *Editorial Director*
Eric Chabrow, *Executive Editor*
Howard Anderson, *Executive Editor*
Tracy Kitten, *Managing Editor*
Upasana Gupta, *Contributing Editor*
Jeffrey Roman, *Associate Editor*

Production

Michael D'Agostino, *Marketing Director*
Glenn H. Mason, *Art Director*
Ian Roberts, *Graphic Designer*

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries. This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

The ISMG Network

BankInfoSecurity
CUInfoSecurity
GovInfoSecurity
HealthcareInfoSecurity
CareersInfoSecurity
DataBreachToday
InfoRiskToday

Contact

4 Independence Way
Princeton, NJ 08540
(800) 944-0401
ISMGcorp.com

Advertising Inquiries:

Nicholas Burke, Sales Director
advertising@ismgcorp.com

Secure your future.



Get the latest news, insights and alerts on career matters of interest to information security **job seekers, employers, educators** and **professionals**.



CAREERS **i**INFO SECURITY®

ENISA Tackles Cybersecurity

Agency Director Helmbrecht on Bridging International Silos

By Tom Field

Because information security threats know no borders, the European Network and Information Security Agency is working hard to ensure the solutions span nations, too, says Prof. Udo Helmbrecht, ENISA's executive director.

"We have the challenge of having 27 member states and 23 official languages, so it's always a challenge to work together and find the same approach," says Helmbrecht, whose office is in Athens. "But this is a situation where we at ENISA are in a good [position]."

Indeed, ENISA is strategically staffed by key members of the various member states, and the agency works with private sector and academic organizations to build consensus with stakeholders. The goal: cybersecurity incident prevention.

In an exclusive interview about cybersecurity challenges in Europe, Prof. Helmbrecht discusses how ENISA is helping to encourage a pan-European approach to cybersecurity.

TOM FIELD: What are some examples of what ENISA is doing to encourage a pan-European approach to cybersecurity?

UDO HELMBRECHT: What we at ENISA are doing is working on the prevention side. This is, giving the member states, industry, the private sector and its citizens some guidance and best practice – like how to behave on the Internet. What does it mean if you are going to cloud computing? We have the challenge of having 27 member states and 23 official languages, so it's always a challenge to work together to find the same approach. But this is a situation where we at ENISA are in a good [position] because we have [representatives] from different member states. We are working together with the private sector and with academia to get input from different stakeholders. By this we are building a community among the European member states and institutions, together with the private sector, to work on prevention aspects for cybersecurity.

Last year we did a pan-European cyber exercise where we got nearly all of the member states of Europe together for a tabletop exercise in our branch office in Athens. This was very successful and showed how Europe can work closely together with a national government computer emergency response team, how to improve communication and find some kind of best practices and how one can support the member states.

FIELD: How is breach notification being handled by the agency and within the member nations?



Udo Helmbrecht

“We have the challenge of having 27 member states and 23 official languages.”

- UDO HELMBRECHT, ENISA

HELMBRECHT: If you look into the European legislative procedure, we have on a European level so-called directives which are then put into national law by the member states. In the case of telecommunication about notification of incidents and data breaches, ENISA has the commission to prepare such directives and if they are assigned by the parliament and the Council then ENISA has the member states implement this. This is one of the tasks we are supporting here, the member states implementing European directives into national law. If you talk about data breach notification, this is something which reflects Article 4 of the Privacy Directive, and we are also working together with the European data protection supervisor to support them. ■

To hear the entire interview, please go to:

<http://www.bankinfosecurity.com/interviews.php?interviewID=1206>

From heightened risks to increased regulations, senior leaders at all levels are pressured to improve their organizations' risk management capabilities.

But no one is showing them how - until now.



NEW WEBINAR!

Risk Management Framework: Learn from NIST

Learn the fundamentals of developing a risk management program from the man who wrote the book on the topic: Ron Ross, computer scientist for the National Institute of Standards and Technology.



Presented by
Ron Ross
National Institute of Standards and Technology

REGISTER NOW!

"PROOF OF ATTENDANCE" CERTIFICATES
ISSUED WHICH MAY BE USED
TOWARD SECURING CPE CREDITS

Register now at BankInfoSecurity.com/Risk-Framework



Careers: Growing the Team

It Isn't Just About Filling Jobs; It's About Fulfilling People

By Upasana Gupta

Alessandro Moretti, information security manager and risk officer at UBS, the global banking and financial services group, finds himself with a staffing challenge. It isn't a matter of filling open positions, but rather helping his existing 150-member staff develop the specialized skills to manage vendor risk and services within the organization.

"We can no longer ignore the risks stemming from the supplier end," Moretti says. "Earlier, we would have just concentrated on the main service providers and built relationships with them, but now our process is to manage operational risk indicators across all 50 vendors."

Moretti's challenge is common among security and risk leaders worldwide. It isn't a matter of filling roles, but rather growing them. IT security jobs are more specialized, and employers demand skills that mirror the types of threats, breaches, regulations and risks these organizations face.

'Can't Go on Experience Alone'

So, how do leaders help their staff evolve and acquire these skill sets in demand? In part, they succeed by focusing more on getting universal players to come in and play multiple roles. Example: Brett Wahlin, the newly-appointed chief security officer at Sony Corp. As Wahlin builds his IT security team, he is largely depending on people who have cross-functional expertise and broad experience.

"Team growth and skill development largely depend on how individuals blend with different groups and add value," he says. "It's important for security engineers and architects to understand how we deal with privacy and compliance issues before they come in and handle vendor and in-house products and systems."

As security becomes a key driver for organizations, new roles, increased legal implications and accountabilities push leaders to adopt new methods of developing their teams. Among the strategies: collaborative workforce, cross-functional training, seeking outside expertise to train staff skills for emerging technologies and the evolving threat landscape.

"You can't just go on certification and their experience alone," says Patricia Titus, chief information security officer at Symantec Corp. "Growing a team is about balancing skill sets and identifying individuals who can integrate and



Alessandro Moretti

"I look for IT security people that have a professional career plan and are able to articulate that effectively."

- ALESSANDRO MORETTI, UBS



“You can’t just go on certification and their experience alone.”

- PATRICIA TITUS, SYMANTEC CORP.

align with the company’s business groups.”

The In-Demand Skills

As they grow their teams’ skill sets, leaders demand specific talents in specialized disciplines

that go beyond an employee’s daily tasks, requiring innovation, ability to analyze patterns, predict trends and handle growing responsibilities. Among the hot disciplines:

Manage Vendor Risk: Moretti, also an advisory board member for (ISC)², focuses on the services aspect of what vendors and suppliers are delivering to UBS and how they need to be managed and integrated within the organization. “We want experts to make sure they understand the operational risk and control frameworks of suppliers and know ways to assess risk and quality of what comes out of this process,” Moretti says.

He has seen these positions evolve, requiring far more innovation today through process modification and stabilization. For example, professionals managing vendor relationships need to address risks stemming from integrating a vendor’s software to the corporate network by ensuring the vendor’s software development life cycle follows security best practices and industry standards and has adequate security built in their products. “A step toward innovation is to work with them and develop technology solutions to address some of these risks,” he says.

Understand Business and IT Risk: Titus at Symantec is currently looking to fill the void created by a few senior staffers that recently left the company. She is looking to support her existing staff of 27 IT security members responsible for security operations globally with additional resources specializing in governance, risk management and audit assessment to take away some of the burden and workload her team currently faces.

“Everywhere, IT security teams are getting fairly integrated with the corporate network and business units, so in my vantage point I am looking for people that are well-rounded and have enough business skills to equate risk into a business impact,” she says.

But for some leaders, seeking senior business and risk expertise among existing staff is a challenge. “It seems to be quite difficult to find people with strong risk management backgrounds in Asia,” says Shrikant Raman, senior manager for information risk and policy at Standard Chartered Bank in Singapore, a multinational financial services company headquartered in London. His team is on the hunt for security people that are thinking about compliance, risk management and ways to enable the business.

“(A) majority of the IT security teams here are comprised of desktop networking support roles and hence a learning curve exists. The problem compounds when the security teams need to understand and act rationally based on the risk appetite of the organization,” Raman says.

These leaders are all looking for a mix of junior, mid-level and senior staffers in their teams such that middle management has proper succession plans in place, leaders can engage in mentoring activities and seek fresh ideas from the more junior professionals.

Growing the Team

Here are four ways in which leaders are helping their teams acquire the skill sets in demand.

Cross-Functional Training: At Symantec, Titus is a big believer in mixing her IT security teams and giving her staff the ability to understand what other team members are doing. “I feel this type of exposure gives team members professional capabilities and exposes them to different situations augmenting their on-the-job learning.”

For instance, having the audit team interact with the incident responders helps auditors understand the different factors they should be looking for while assessing IT security controls within the organization. “It happens more frequently than I realize,” Titus says. “Cross-functional training enhances the ability of my team to see across boundaries, which is critical.”

Partner with Professional and Academic Communities: Moretti spends substantial time with professional associations like the International Information Systems Security Certification Consortium, Inc. (ISC)² and the Information Systems Security Association (ISSA). He leverages their partnership with universities and colleges in reaching out to people starting their careers in information security to help them adopt a more broadened career path, which ends up in specialization within a particular discipline. “It is significant to interact with universities, articulate our understanding to those setting out on their careers and modify study modules to build the foundation for a prepared future.”

Engage in Brainstorming Sessions: As Wahlin builds his team at Sony, he is looking to approach problem-solving and skill development in a new way. “We have conversations at least once a week where we talk about what-if scenarios - what if this happened? How would we approach the issue?” he says. He finds these sessions fruitful in engaging employees to foresee future trends and opportunities. “So far it’s been a great avenue to help my team think independently and open their mindset to do things differently.”

Seek Industry Subject Matter Experts: At Standard Chartered bank, Raman has a comprehensive training program that includes sessions with specialized subject matter experts representing technology companies such as Splunk and Trusteer. Also, they have an internal risk forum within the bank that meets weekly to discuss and brainstorm ideas on risk mitigation, identifying attacks and vulnerabilities, etc. “These sessions help people to get exposure to other lines of thinking and broaden their ability to get new ideas,” Raman says. ■

Upasana Gupta is a contributing editor to Information Security Media Group and manages CareersInfoSecurity.

Is educating top business and government leaders scaring them to act? Yes. Is that a good thing? Yes.

A Wake-Up Call for Risk Management

By Eric Chabrow

The slew of data breaches over the past year has raised the consciousness among businesses and governments of the need to manage risk more than ever before. Breaches, simply, have an adverse impact on the fundamental operations of a business or government and without fully understanding that, executives and managers cannot smartly run their operations successfully.

Among the most publicized - and embarrassing - breaches was a common missing link: the lack of a senior-level, technology-savvy business leader who could explain to top executives the risk the organization faces by not taking the proper precautions to safeguard their information assets. Neither security provider RSA nor entertainment conglomerate Sony had a chief information security officer on duty when both companies fell victim to separate breaches last spring. Since then, both companies have named highly respected information security professionals as their CISOs: Eddie Schwartz at RSA and Philip Reitingger at Sony.

"You need a CISO today to manage not only the IT risks, but understand and influence the business risks that are imposed on the company by the decisions and strategies it takes," says John South, CISO at Heartland Payment Systems, the U.S.-based payment processor that experienced a highly-publicized breach in 2009.

The impact on the business at RSA was far different from that of Sony, but in both cases, the breaches struck at their core offerings. The RSA breach exposed the secret code of its SecurID multifactor authentication token, raising questions among customers whether

the product would function as promised. At Sony, the breach brought down its PlayStation and Qriocity online services for weeks and bared the personally identifiable information of tens of millions of customers. In the wake of the breaches, both companies realized a gap existed in their respective approaches to understanding the risks their businesses faced by not having a CISO.

Both breaches have been costly. The RSA breach cost parent company EMC at least \$66.3 million. Sony pegged its losses to the breach at 14 million yen, which in October 2011 equaled more than \$180 million.

Reputation Risk and Large Dollar Losses

A Ponemon Institute study measured the cost of a breach at \$214 for each record, an amount that quickly grows when hundreds of thousands and millions of records are exposed. "The commercial challenge is the most pressing concern, thanks to the combination of reputation risk and large dollar losses," says Julie Conroy McNelley, a fraud analyst with Aite, a U.S.-based financial research and consulting firm to banks.



Being breached - especially one that highlights an enterprise's vulnerabilities - means companies must confront the reality that inadequately protecting their information technology could have a significant, adverse impact on their finances and the value of its publicly traded shares. Last May, Michaels Stores uncovered that point-of-sale pads at 90 of its crafts stores in 20 states that customers use to key in their personal identification numbers were tampered with, potentially resulting in customer debit and credit card information being compromised. At least three class-action lawsuits have been filed by consumers, which, depending on their outcome, could have a despicable impact on Michaels' bottom line.

Michaels does not contend its IT security is inadequate - indeed, it has said it has taken steps to mitigate such future breaches. But the retailer concedes in what could be described as boilerplate statements in a filing with the Securities and Exchange Commission that unforeseen circumstances could result in its failure to adequately maintain security and prevent unauthorized access to electronic and other confidential information and data breaches, such as the repayment card terminal tampering, could materially adversely affect its financial health.

Communicating Risks to Top Management

Communicating risks to top management is becoming a key responsibility of CISOs. "After we did the executive briefing, we had a much stronger uptake with agencies who said, 'Please tell me how I can improve our compliance with the policy,'" says New York State Cybersecurity Director Tom Smith. "Help me get the regular training. Help me move my information classification process forward.' ... There is a clear understanding among the agency commissioners that they want to address those risks before they are the ones who have the breach that's discussed in the news. There is a higher sensitivity to it. I think they are learning the message and the importance of being involved in this process."

Is educating top business and government leaders scaring them to act? Yes. Is that a good thing? Yes.

"If I'm worried about something, I might actually want to do something about it and take some action," says Patricia Titus, who left IT services provider Unisys to become Symantec's CISO late last year.

A fundamental reality is that breaches will occur. Recognizing that, businesses must comprehend that information risk management will help mitigate damage from attacks. "I don't know that you can fully prevent breaches," says Malcolm Harkins, chief information security officer at chipmaker Intel. "The fact of the matter is that it is a risk management issue."

"You can manage risk and mitigate risk, but you can not eliminate risks. That is just one mind set that has to be changed. How do you manage the risk and how do you mitigate the risks such that to some extent you can live with some level of potential compromise? It will occur. There are a number of things people can step back and consider regarding how to approach this when they think about managing those risks."

Intel, a few years back, shifted its information risk management strategy toward a concept that people are the new perimeter because of mobility, interaction among third parties and social computing, factors that affect how business functions. "Even if you had completely secure systems, you could still have an incident because an individual shared too much information and maybe by mistake disclosed some sensitive information that then causes an issue for a company," Harkins says.

'Typical' Awareness Training Doesn't Cut It

Indeed, people - employees and contractors - play a crucial role in information risk management if they know what to do. Too often, though, organizations don't allot the resources to make employees aware of the risks that could expose information assets to a breach. "The typical five minutes of annual training on information security and privacy that most healthcare organizations provide is just not cutting it," says healthcare security consultant Tom Walsh.

The wave in breaches forces organizations to take a more holistic view of risk

"The typical five minutes of annual training on information security and privacy that most healthcare organizations provide is just not cutting it."

- TOM WALSH, SECURITY CONSULTANT

rather than react with a knee-jerk response. "The first reaction always is to go and put up big, big walls and stop people from getting in every time we see one of these breaches," says Robert Stroud, vice president of service management and governance at enterprise software vendor CA Technologies and international vice president of ISACA, an IT association that encourages the use of best practices.

"For risk managers, it's the very nature of their role," Stroud says. "They need to understand the potential risk of any breach. Some breaches will have minimal impact on the business and

some breaches may just be embarrassing and have some major impact. As risk managers, we've got to focus on that key information and data that we need to protect. We need to identify that to the organization. We need to clearly articulate that to the organization. Finally, we need to ensure that we help the organization put appropriate safeguards around that information, because at the end of the day really it's all about the data."

When evaluating threats, organizations must evaluate the various aspects that make up a business. "Our most critical vulnerabilities are the ones that can potentially bypass our technical enforcements," says Anthony Vitale, vice president of information technology development for Patelco Credit Union in the U.S. Gartner analyst Avivah Litan says technology is just one leg of a three-pronged solution. "The other two equally important prongs are operations and strategy," she says. "Many breaches were accompanied by alerts that went off during the breach, but no one was paying attention to the alerts and alarms. ... People and processes can be showstoppers, even with the best technology."

But security awareness can go only so far, especially when dealing with customers. Matt Speare, who oversees security for M&T Bancorp, says the Buffalo, N.Y., bank company remains very concerned about customer vulnerabilities to cyberattack. "The odds are stacked against them having adequate controls to protect themselves," he says. "Despite our best efforts for awareness and education, they continue to make rudimentary mistakes, which put them at risk for exploitation." (Continued on p. 14)



Tom Walsh

Top 10 Breaches of 2011

A string of data breaches in 2011 put the spotlight on the need to take adequate precautions to protect sensitive information. From hackers issuing phony digital certificates to millions of patients having their records potentially exposed as a result of lost or stolen backup files, breaches point to the value of preventive measures, ranging from encryption to intrusion detection.

1. DigiNotar

The September 2011 breach of certificate authority DigiNotar could prove to be among the worst Internet security events ever. Hackers stole the private key used by the Dutch company to assure the trustworthiness of the digital certificates it issued to website operators. Employing the stolen private key, the hackers issued counterfeit certificates aimed at fooling visitors into believing that sham websites they mistakenly accessed were the ones they actually intended to visit.

2. RSA

A well-crafted e-mail with the subject line “2011 Recruitment Plan” tricked an RSA employee to retrieve from a junk-mail folder and open a message containing a virus that led to a sophisticated attack on the security company’s information systems. In the March 2011 incident, the attacker targeted RSA’s SecurID two-factor authentication product in what the security vendor termed an “advanced persistent threat” breach.

3. Sony

Distributed denial-of-service attacks in April 2011 that crippled Sony Corp.’s PlayStation gaming network and Qriocity music service camouflaged simultaneous intrusions that resulted in the exposure of personal identifiable information, including credit card information, from as many as 77 million customer accounts.

4. Hacktivists

With regularity throughout 2011, members of the so-called “hacktivist” groups Anonymous and LulzSec performed a virtual version of vandalism on well-known private and government websites. They did not cause major damage, but exposed personally identifiable information and, at times, embarrassing details about individuals’ computer hygiene. Among their victims: Fox, Infragard, PBS, the U.S. Senate and Sony.

5. TRICARE

About 4.9 million individuals enrolled in the U.S. military’s TRICARE health program were affected in this breach, reported in September 2011. The incident involved backup tapes stolen from the car of an employee of a TRICARE business associate, Science Applications International Corp.

6. UBS

Switzerland-based UBS, a global financial services firm, reported in September 2011 a \$2.3 billion loss linked to unauthorized trades conducted by a trader in its Global Synthetic Equity business in London.

7. Sutter Health

Sutter Health, a California health system, faces two class action lawsuits in the wake of a breach involving the theft of an unencrypted desktop computer containing information on 4.2 million patients. The stolen computer contained two databases, one with more extensive information about patients.



8. Pentagon

Hackers believed to be backed by an unidentified nation obtained 24,000 Pentagon files related to systems being developed for the U.S. Defense Department during a single intrusion in March 2011, one of the worst digital attacks against the DoD.

9. Health Net

This health insurance company notified 1.9 million individuals nationwide that their healthcare and personal information may have been breached in January 2011 as a result of nine server drives that were discovered to be missing from a California data center managed by IBM.

10. Michaels Stores

Michaels Stores in May 2011 identified a scheme that targeted its point-of-sale devices in nearly 90 U.S. stores. Legitimate PIN pads were swapped for PIN pads manipulated to skim and collect card details, such as personal identification numbers. The breach was first identified by card issuers, which quickly found Michaels purchases to be the common denominator among all of the cardholders who were reporting debit and credit fraud.

Top 5 U.S. Healthcare Breaches of 2011

U.S. healthcare organizations must report breaches to federal authorities. *The Department of Health and Human Services' Office for Civil Rights* compiles what's become known as the "wall of shame" on its website, listing major incidents as the details are confirmed. Here's a look at 2011's biggest healthcare breaches, in terms of the number of individuals affected.



1. TRICARE

Congress is investigating the September breach affecting 4.9 million beneficiaries of TRICARE, when unencrypted backup tapes were stolen from the parked car of an employee of Science Applications International Corp., a business associate of the military healthcare program.

The TRICARE incident is the largest breach reported to federal authorities so far under the HIPAA breach notification rule, which went into effect in September 2009.

2. Sutter Health

The California integrated delivery system faces two class action lawsuits in the wake of an October breach involving the theft of an unencrypted desktop computer containing information on 4.2 million patients.

The stolen computer contained a database for Sutter Physician Services, which provides billing and other administrative services for 21 Sutter units. That database held limited demographic information on about 3.3 million patients collected from 1995 through January 2011. The device also contained a database with more extensive information on 943,000 Sutter Medical Foundation patients, dating from January 2005 to January 2011. This smaller database also included dates of service and a description of diagnoses and/or procedures.

3. Health Net

Federal authorities plus at least four state agencies launched investigations of a breach affecting 1.9 enrollees of insurer Health Net. A class action lawsuit was filed in the case, which involved nine server drives that were discovered missing in January from a California data center managed by IBM. In 2009, Health Net reported another breach affecting 1.5 million nationwide that involved the loss of a computer disk drive. That case resulted in three state fines.

4. Nemours

The children's health system offered about 1.6 million individuals one year's worth of free credit monitoring and identity theft protection following an August breach incident stemming from the loss of three unencrypted backup tapes.

Patient billing and employee payroll information on the tapes, missing from its Wilmington, Del., facility included names, addresses, birth dates, Social Security numbers and information about insurance, medical treatments and direct deposit bank accounts. The backup tapes were stored in a locked cabinet, which were reported missing Sept. 8. They are believed to have been removed a month earlier during a remodeling project.

5. Eisenhower Medical Center

The Rancho Mirage, Calif., hospital notified more than 514,000 patients of a March breach of a limited amount of personal information stemming from the theft of an unencrypted computer. The computer contained a patient index backup file that included patient names, ages, dates of birth, the last four digits of Social Security numbers and the hospital's medical records numbers. It did not contain health or financial information.

(Continued from p. 12)

“Many breaches were accompanied by alerts that went off during the breach, but no one was paying attention.”

- AVIVAH LITAN, GARTNER ANALYST

It Can Happen to You

Customer vulnerability to attacks erodes trust in the business, a valuable asset that must be balanced with other factors in determining what risks an organization must take to mitigate breaches.

But Symantec's Titus says that for too many organizations the lessons from breaches that occurred to RSA and Sony will not be heeded until such attacks occur to them. "I don't know that it will stop a lot of people until it happens to them. Unfortunately a lot of people read about things happening and don't think it's going to happen to them," says Titus, the onetime CISO at the Transportation Security Administration, the federal agency charged with protecting the nation's airports. "What is the fallout from the Sony breach and are people going to hold their breath and wait and see what happens or are they going to proactively go and take action? And are the institutions actually going to help people understand what protections they could put in place for themselves?"

It's a concern echoed by Intel's Harkins: "The thing I worry about with all of these breaches is that companies, individuals and users start shying away from technology and the productive use of it. The best way to shape risk is to sometimes run toward the risk of your assets. I believe my mission at Intel, and more broadly information security's mission in any organization, should be protecting to enable.

"If we are not enabling the use of the information, then the organization can't get the value. That's why I think it's a risk management thing. That's why I think there's a lot of balancing of items. As much as organizations look to prevent, detection is a big area that they need to focus on. And certainly response needs to be a prepared critical control for what I think is inevitable in terms of potential breaches or intrusions into people's computer environments." ■

(Howard Anderson contributed to this story.)

Using Anomaly Detection to Prevent Online & Mobile Banking Fraud

The FFIEC Guidance Supplement issued in June 2011 put anomaly detection in the spotlight and generated significant interest in anomaly detection solutions. It also created some confusion.

As market leaders in anomaly detection solutions, we at Guardian Analytics are often asked to explain what the FFIEC wants. This article answers two key questions that we're asked every day:

What is anomaly detection?

How does anomaly detection work to stop online banking fraud attacks?

Sophisticated Fraud Attacks Are Getting Past Today's Defenses

Today's fraudsters are professional criminal gangs that are continually developing innovative ways to defeat financial institutions' defenses. Internal researchers at Guardian Analytics are constantly evaluating attacks across more than 100 financial institutions and regularly releasing their findings.

Some recent examples include:

- Fraudsters targeting online banking platforms instead of individual accounts, enabling them to attack multiple institutions simultaneously and expand attacks to include smaller institutions
- Automated Transfer Systems (ATS) malware that automatically initiates or modifies transfers during a victim's online banking session, effectively eliminating the need for human involvement.
- Fraud attacks featuring wire transfers to high-end jewelry stores with DDoS attacks that act as a smoke screen, eliminating the need for mule accounts into which funds are transferred.

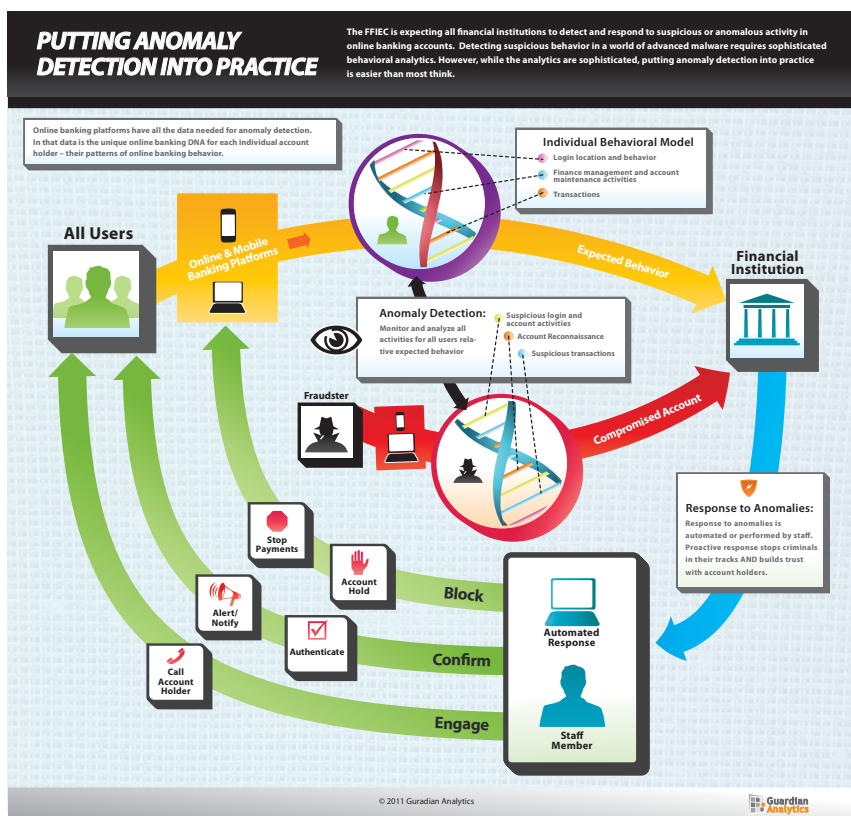
These examples highlight the innovation and sophistication of attacks that caused the FFIEC to act. The Guidance went on to say that "anomaly detection and response could have prevented many of the frauds" that the FFIEC studied in preparing the Supplement.

What is Anomaly Detection?

Anomaly detection is a technique that compares online behavior with established patterns of legitimate behavior and looks for anomalies. The most effective form of anomaly detection uses "behavioral analytics" to monitor every individual account holder instead of comparing behavior to generalized population-level standards. (See the [Anomaly Detection Toolkit](#) for additional details.)

How does Anomaly Detection Work?

Each account holder has a unique online banking fingerprint or DNA. Anomaly detection creates a behavior profile of every user and then uses it to decide if behavior during *this* session is normal for *this* user. Fraud typically takes place over a period of time and a number of online sessions. Anomaly detection builds a cumulative risk score across all online sessions over time to determine when fraud is likely taking place.



Anomaly detection solutions compare current behavior to established online DNA for every user. ([download Anomaly Detection infographic](#))

To learn more about anomaly detection and FraudMAP from Guardian Analytics that over 120 banks and credit unions are using to stop fraud every day, please go to www.GuardianAnalytics.com.

BYOD

BRING YOUR OWN DEVICE

BYOD

How to Minimize Risk

By HOWARD ANDERSON

When it comes to mobile devices, accommodating BYOD, or bring your own device, is a fact of life for organizations in all industry sectors worldwide. So, what can information security professionals do to minimize the risks involved in enabling staff members to use personally-owned tablets, smart phones, USB drives and other mobile devices for business purposes?



It all boils down to this: Conduct an inventory of all the types of personally-owned devices employees want to use for work-related tasks. Take every possible step to apply as many of the same precautions to these personally-owned devices as you apply to corporate-owned devices. And be sure to enter a clearly spelled out legal agreement with those who use personal devices for work-related purposes, then provide them with extensive ongoing training.

Whether overall security risks increase or decrease by accommodating BYOD “is probably a moot point,” says Christopher Buse, chief information security officer for the State of Minnesota. “BYOD is already happening, and the trend will surely continue because that is what people want.”

Vishal Salvi, chief information security officer at HDFC Bank in India, agrees that the BYOD trend is here to stay. “But the success of BYOD programs will depend on how security leaders handle complex issues of trust and liability resulting from the shifting ownership of mobile devices,” he stresses.

Balancing Risks, Benefits

Accommodating personally owned tablets, smart phones, USB drives and other mobile devices brings risks. The devices are easily lost, which can make any data stored on them vulnerable. And unless organizations make a concerted effort to make sure security controls, such as encryption and remote-wipe capability, are in place on these devices, they could be much riskier to use than corporate-owned devices, which routinely have security controls installed.

But BYOD also can yield substantial benefits, not the least of which is hefty cost savings (see: Five Benefits of BYOD, p. 19).

Faced with limited government funding, the U.S. Department of Veterans Affairs, for example, couldn’t afford to provide a smart phone or tablet to everyone on staff who wants to use one, acknowledges Roger Baker, CIO. He expects mobile devices eventually will replace desktop computers, dramatically decreasing the VA’s costs while increasing user convenience.

Some experts argue that those who own the mobile devices they use for business purposes are more motivated to protect them and the information they contain.

“If there are pictures of your kid’s birthday party on your iPhone, you’re going to keep tighter control of it compared to just another corporate device,” argues Malcolm Harkins, chief information security officer at Intel Corp. “Allowing personal ownership and use will go a long way in getting users to protect the device.”

Legal Agreement

Because of overwhelming demand, the VA, which provides healthcare to veterans, recently began accommodating the use of corporate-owned iPads and iPhones in addition to BlackBerries and laptops. The VA will gradually accommodate personally owned Apple devices in 2012, at first allowing the devices to be used only for viewing, and not storing, patient information. Eventually, the VA expects to accommodate devices running the Android operating system as well.

The security issues involved when allowing personally-owned devices are legal, rather than technical, Baker contends. “We’re establishing what it is we need to have the user sign, relative to their personally owned device, that will ensure, for example, that I have the right to wipe any VA information off of it at my discretion ... and ensure that I have the right to access the device to review it as needed.”


Baker says the key issue is “what level of control do we need to have, as the government, in order to ensure that all the right things are happening with the device when it connects to us or when it contains veterans’ information.”

An effective way to enforce mobile device security strategies is using a mobile device manager application to monitor all devices, no matter who owns them, some experts say (see: How to Enforce Your Mobile Policy, p. 21). That’s the approach the VA is taking.

Security Controls

Requiring the use of specific security controls on personally owned mobile devices can lead some workers to forego BYOD.

For example, about half of the Delaware state employees who had been using their mobile devices to access the state network opted not to use them once the state required added security measures about a year ago, notes Elayne Starkey, the state’s chief security officer. “If I used to have unfettered access to the state



“If there are pictures of your kid’s birthday party on your iPhone, you’re going to keep tighter control of it compared to just another corporate device.”

- MALCOLM HARKINS, CISO, INTEL CORP.



Roger Baker, CIO of the U.S. Department of Veterans Affairs, expects mobile devices eventually will replace desktop computers, dramatically decreasing the VA's costs while increasing user convenience.

network and now I have to jump through a couple hoops to continue that access, I'm just not going to go to the trouble," she says, voicing the thoughts of some state workers. "I'm just not going to continue to be maybe as diligent about keeping up with my e-mail in the evening hours. I'll wait until 8 the next morning."

Until late 2010, Delaware state employees could access remotely - with few restrictions - government IT systems using their own iPhones, Androids and BlackBerries. "That was the piece that was keeping me up at night," Starkey says. "It was kind of an oversight on our part, more or less. We had not locked that down as tightly as we should have. In the beginning, it was not such an issue, but as the smart phones became more and more popular, we found that the number of devices accessing the state network was continuing to grow."

Starkey didn't want to ban the use of personally owned devices for conducting state business; she recognizes that many state employees want to use a single

5 Benefits of BYOD

Reasons to Accommodate Personally-Owned Mobile Devices

Although accommodating the use of personally-owned mobile devices for business purposes has risks, advocates say the "bring your own device" trend can bring substantial benefits. Those may include:

1. Cost Savings

If employees can use their own devices, businesses can forgo the cost of acquiring the hardware, which can result in substantial savings.

For example, the Indian bank HDFC has slashed its total computer hardware costs in the two years since it introduced its bring-your-own-device program, says Vishal Salvi, chief information security officer. The bank, which used to rent certain mobile devices for its employees, now requires those who want to use mobile devices to acquire them on their own. The bank is attempting to outsource support for the devices to further control costs.

2. Better Protection

In the last two years, as BYOD users have increased to about 30,000 at chip-maker Intel Corp., incidents of lost and stolen devices have dramatically decreased, says Malcolm Harkins, chief information security officer at Intel Corp. "People typically take better care of their personal assets," he notes.

3. Improved Morale

Enabling staff members to use their own mobile devices for work-related purposes can be a morale booster. "Employee flexibility is what BYOD is all about - letting employees have their own thing, their own way and enhancing their comfort level at work," says Luke Forsyth, European vice president of IT security services at CA Technologies.

4. Better Agility, Resiliency

Smart phones and other mobile devices can play an important role in disaster recovery. Harkins recently conducted a disaster preparedness drill for Intel that simulated an earthquake damaging a data center. "We more than doubled the coordination and communication efforts with smart phones," he contends. That's because employees with smart phones were reachable during off hours and able to communicate with each other and follow Intel's contingency planning for the worst possible scenarios, he says.

5. Improved Productivity

If more employees use mobile devices for business purposes, thanks to BYOD, employee productivity can improve. "Tablets are creating an additional work space in an employee's day, which is typically off hours," Salvi says. The devices also make it easier to work while traveling, he adds.

"The boundaries of an employee's work and home life have blurred to the point where it is becoming increasingly difficult to have completely distinct sets of tools for home and work," says Christopher Buse, chief information security officer for the State of Minnesota. "We should approach this BYOD trend with an 'embrace and educate' philosophy and leverage the benefits it offers."

What can information security professionals do to minimize the risks involved in enabling staff members to use personally-owned devices?

device for personal and business purposes. The solution was to place controls on the personal devices that would help ensure the safety of the state IT system. The seven controls Delaware requires are:

- Strong password;
- Password history;
- Password that expires;
- Inactivity time out;
- Lock out after seven failed attempts to log on;
- Remote wipe if the device is compromised or after seven consecutive failed log-on tries;
- Encryption, if devices are capable of employing it.

“We’re not trying to be difficult; we’re not trying to impose rules,” Starkey says. “But we are working to ... prevent data leakage and data loss out of the state network.”

To Store, or Not to Store?

One major issue when using either corporate-owned or personally owned devices is whether to permit storage of sensitive information on the devices.

Over the long haul, it could prove impractical to limit data storage, says security consultant Rebecca Herold. Although allowing the use of personally-owned devices solely for viewing sensitive information, such as medical records, is a good security measure, “I believe there will be a lot of pushback” regarding such a policy, she says. “Once personnel are allowed to use their own mobile computers, they will want, and actually expect, that they can use them in all the same ways as the entity-owned devices,” she says.

But if sensitive information, is, indeed, stored on personally-owned devices, it must be protected with encryption, stresses Herold, who heads the consulting firm Rebecca Herold & Associates.

Some mobile devices, however, cannot accommodate full disk-level encryption. That’s why certain organizations are requiring any stored data to reside within specific applications that can accommodate appropriate encryption. For example, that’s the approach the VA is taking for iPhones and iPads.

A Mobile Policy Enforcement Checklist

Key Steps for Keeping Mobile Devices Secure



Terrell Herzig, a mobile device security thought leader who is information security officer at UAB Health System in Birmingham, Ala., offers a checklist of mobile device security policy enforcement tips. His advice is based on the steps his organization is taking.

Leverage Your Inventory Tools

Many organizations use IT inventory tools that scan and inventory software, hardware and port usage of computer assets. If your organization has such a tool, consider getting a routine report that can identify device and port usage metrics.

If your organization doesn’t have access to an asset inventory tool, consider purchasing one that will, at a minimum, report USB port usage and CD/DVD Rom activity and that offers the capability to shadow the data transferred among these devices. Routinely enable the shadowing feature and review the data to gain an understanding of what data are being utilized on the device.

Use Mobile Device Management

Consider purchasing mobile device management software that will help enforce your mobile policies. This will enable mapping use cases directly to policy profiles that can be continuously managed. If a mobile device does not comply with a policy, arrange to have it automatically wiped of data.

Create BYOD Guidelines

If your organization allows the use of personal devices for business purposes, make it a condition of participation in the corporate environment that the devices run the same security tools as corporate devices, with a profile that matches their use case. Have users sign a document confirming the expectations outlined in the mobile device policy and the impact for noncompliance. Use this as an opportunity to educate.

Run Frequent Reports

Run frequent reports using the tools described and take action where appropriate. Make sure policies spell out appropriate remediation steps in the event a device fails to adhere to the policy.

Importance of Education

Education and ongoing awareness training play key roles in ensuring that a mobile device security policy is actually followed by the rank and file, whether they’re using corporate-owned or personally owned devices, Herold contends.

That training should address a wide range of issues, including when and how to use encryption, how to back up sensitive information and how to use anti-malware software.

Despite the risks involved, accommodating BYOD is part of doing business in the 21st century, Herold and other security experts acknowledge.

“You should allow employees to bring their own devices,” says Bill Wansley, who oversees multidisciplinary teams at the consultancy Booz Allen Hamilton. “It’s a trend that organizations need to embrace.”

But in embracing the trend, Wansley says, executives must “think about their policies and procedures and what potential risks they may be bringing on to their enterprise, unwittingly, and what they can do to help mitigate that risk.”

How to Enforce Your Mobile Policy

A comprehensive mobile security policy is essential now that so many employees in so many industries worldwide use tablets, smart phones, USB drives and a long list of other mobile devices and media. But a policy doesn't do much good unless it's adequately enforced.

Key components of an enforcement strategy include using a mobile device manager application to monitor devices, entering legal agreements with those using personally owned devices and repeatedly communicating security expectations.

Mobile Device Manager

Effective enforcement of a mobile device security policy requires the use of a mobile device manager application that closely monitors the devices and enforces security controls, says Stephen Warren, principal deputy CIO at the U.S. Department of Veterans Affairs. The VA, which provides healthcare to veterans, is in the process of acquiring an enhanced mobile device manager, he adds.

Roger Baker, the VA's CIO, noted in October that the VA expects to accommodate the use of more than 100,000 iPads and iPhones within 18 months, including a mix of government-owned and personally owned mobile devices.

"We certainly will ... exercise the ability to [remotely] wipe devices if we determine ... that we don't know that [a device] is with its authorized user," Baker said. "And that's part of the mobile device manager's [function]. The mobile device manager, in particular, will manage which devices have been authorized to connect to our network. It will verify that no software that we believe causes any kind of compromise to the device is there."

The mobile device manager "is going to play a pretty critical role for us," Baker stressed. "Every device, before it's allowed to connect to the network, will go through the MDM, and the MDM will verify that the device is only running software that we have approved and that all the policies on the device are still implemented as they're specified to be for access to the network."

UAB Health System in Birmingham, Ala., also uses a mobile device manager to help enforce its mobile policies (see: A Mobile Device Enforcement Checklist, p. 20).

User Agreements

A key to enforcing security policies for those using personally owned devices is having the users sign legal documents "that will ensure, for example, I have the right to wipe any VA information off the device at my discretion," Baker says. "It will also ensure that if the device needs to be looked at for some reason, we will have access to it."

The VA also will use its mobile device manager application to monitor personally owned devices just as it does for VA-owned devices.

Like the VA, the state of Delaware requires employees who want to use their own devices for work to sign a detailed agreement.

First, employees go to a website to complete an online form requesting their managers' approval for access rights. "We want to know that there is a true business need for that connection," says Elayne Starkey, the state's chief security officer. Once their use of a personally-owned device to access the state network is approved, employees must digitally sign an agreement to have seven security controls placed on their devices - the same controls that are used on corporate-owned mobile hardware. Those controls include agreeing to allow the remote wiping of data from the device if it's compromised or in the case of seven consecutive failed log-on attempts.

"We don't need to physically touch the device," she says. "We can configure that device remotely and push the seven security controls out to their device. Then, the next time they connect, all of the new security controls are in place."



Elayne Starkey

"We don't need to physically touch the device. We can configure that device remotely."

- ELAYNE STARKEY, CSO, STATE OF DELAWARE

Communicating Expectations

Information security consultant Rebecca Herold says education and ongoing awareness training play key roles in ensuring that a mobile device security policy is actually followed by the rank and file. She stresses that a practical, enforceable mobile policy must cover "the use of both entity-owned and personally owned mobile devices."

At Intel Corp., ongoing communication is an important component of mobile policy enforcement efforts, says Malcolm Harkins, chief information security officer.

Policies and security expectations, which are the same for corporate-owned and personally owned devices, are communicated:

- When employees sign up for particular services;
- When staff connect a new device to the Intel network;
- On a regular basis through security awareness articles and notices;
- In an annual security refresher for the entire staff. ■

(Howard Anderson, Eric Chabrow, Tracy Kitten, Upasana Gupta, and Jeffrey Roman contributed to this story.)

BYOD: “It’s Going to Happen”

Intel’s CISO on How to Manage the Risks of Mobility

By Tom Field

It’s not a question of if employees will bring their own mobile devices to work and connect to your systems. It’s a matter of when. And you’d better have a policy when it happens, says Malcolm Harkins, CISO of Intel.

“It’s going to happen because everybody has [mobile devices] in their pockets today,” says Harkins, who has overseen Intel’s global BYOD initiative.

At Intel, the BYOD trend started about two years ago, and Harkins was quick to embrace it as a means to cut costs and improve productivity. Since Jan. 2010, the number of employee-owned mobile devices has tripled from 10,000 to 30,000, and by 2014 Harkins expects that 70 percent of Intel employees will be using their own devices for at least part of their job.

His advice to organizations just now struggling with BYOD: “Don’t shy away from the risk issues. Figure out how to run to the risk to shape it.”

In an exclusive interview about BYOD, Harkins discusses advice for organizations struggling with BYOD.

Harkins is vice president of Intel’s Information Technology Group and CISO and general manager of information risk and security. The group is responsible for managing the risk, controls, privacy, security and other related compliance activities for all of Intel’s information assets.

TOM FIELD: What’s the argument for employees bringing their own devices, versus the company issuing mobile devices?

MALCOLM HARKINS: I think the argument for BYOD in my mind is, simply put, they’re already bringing them into your enterprise; the question is whether or not they’re hooking them up. Whether or not they’re hooking them up and taking information onto those devices in a way that actually is unmanaged risk. Or are you just not getting the benefit of it, and the employee is not getting the benefit of the device that’s in their pocket? I think we saw this with the tremendous growth; by just enabling it, we more than doubled the amount of small form-factor devices in use.

Now I still think there’s always going to be an argument for some company-issued devices, whether it be because we need full oversight across everything on the device for data protection or other compliance purposes, or if somebody’s job category really does require them to always be on, always connected, always reachable. It makes – to some extent – a lot of business sense that the company would incur the cost to provide that capability. And so I think you’re going to end up in this model where it’s relatively mixed.



Malcolm Harkins

FIELD: For organizations that are now or soon will be struggling with this whole concept of BYOD, what advice would you offer to them?

HARKINS: Don’t shy away from the risk issues. If you ignore it, you’re going to have the risk, and it’s going to be bigger than if you go and be in front of it. I think the other thing – beyond just the traditional information security or privacy and those types of control and compliance requirements that I think an IT organization and my peers normally contemplate – go engage other parts of your business [such as] the HR team, the HR legal team. Explore the wage and hour risk issues of hourly employees, explore employment law issues in different areas, and look at it across the geographies you’re in, because each geography has slightly different legal and regulatory requirements. Go do that so you don’t encounter an issue because you didn’t think far enough or broad enough about the risk considerations beyond just the obvious data protection ones. ■

To read the entire interview, please visit:
http://www.bankinfosecurity.com/articles.php?art_id=4394

Need strong 2-factor logon or transaction authentication that works the same way for mobile and desktop users?

Authentify has an app for that!



New Authentify 2CHK™ delivers strong out-of-band authentication and a consistent user experience across all of your user's mobile or stationary computing devices.

Your users or employees have many options for accessing online, networked or cloud-based resources. Authentify 2CHK™ (pronounced “two check”) enables you to easily add a strong 2-factor authentication layer across all of their mobile and fixed endpoints. No more authentication gaps for you, no more headaches for your end users.

2CHK™ is the next generation out-of-band authentication service from phone-based authentication leader Authentify. The user interface is a small and intuitive app for smart phones, tablets, laptops and desktops. 2CHK enables you to defeat key logging, MITM and other forms of advanced exploits.

Visit Authentify at: Booth # 832 at the RSA Conference Expo

- The Authentify 2CHK™ app supported on smartphones, tablets, desktops and laptops.
- An authentication process for logon or transaction verification that is convenient and natural for the end user.



www.authentify.com

Email: info@authentify.com • Voice: 773-243-0329 • Text: 847-313-5531

Roadmap to Securing Online Transactions

What Every Leader Can Learn from the FFIEC Authentication Guidance

By Tracy Kitten

In response to the evolving threat landscape, U.S. banking regulators in 2011 released an update to their 2005 online banking authentication guidance. This update from the Federal Financial Institutions Examination Council, known as the FFIEC Authentication Guidance, basically spells out that banking institutions should:

- Conduct periodic risk assessments;
- Deploy layered security controls in the transaction process;
- Improve customer awareness efforts.

And while this guidance is aimed specifically at financial institutions, the recommended processes and controls are applicable to most global entities in their online transactions. Here's an overview of the FFIEC Authentication Guidance and its key lessons for any organization.

1. Periodic Risk Assessments

The risk assessment is the building block of any information security and risk management program. And increasingly global regulatory bodies are calling upon their entities to perform regular risk assessments (Ex: the Reserve Bank of India's 2011 banking guidance).

The FFIEC's original 2005 guidance called for periodic risk assessments, but few institutions committed themselves to that goal. The updated guidance now calls for a minimum of annual risk assessments, so that customer authentication controls can be adjusted and updated as new threats are identified. These risk assessments should review:

- Changes to the internal and external threat environment;
- Changes in the customer base;
- Changes in customer-facing functionality offered through online channels;
- Incidents of security breaches, identity theft or fraud experienced by the institution or industry.



As critical as risk assessments are to any risk mitigation process, they frequently are overlooked by organizations. And here is where non-banking entities can take a page from the FFIEC Authentication Guidance, says Gartner analyst and financial fraud expert Avivah Litan.

“Businesses in other sectors should take this lesson from the FFIEC playbook, and certainly not take for granted that they understand their risks without going through the formal process of an annual risk assessment,” she says.

2. Layered Security Controls

The updated guidance was influenced in part by a wave of corporate account takeover incidents that struck banking institutions and their commercial customers. Essentially, the customers' banking credentials were stolen via social engineering and malware, and then the commercial banking accounts were compromised via fraudulent ACH and wire transactions.

In issuing the guidance, banking regulators were critical of institutions for not detecting and preventing these fraud incidents, and so they prescribed a layered approach to security for high-risk Internet-based systems. The guidance further defines layered security as being a process that relies on different controls at different points in a transaction. With a layered approach, the weakness in one control is compensated for by the strength of a different control. At minimum,



Avivah Litan

“[Customers] need to participate in the solution – and not just in the problem.”

- AVIVAH LITAN, GARTNER

The message from the FFIEC is clear and applies to any organization that manages online transactions: “Since virtually every authentication technique can be compromised, financial institutions should not rely solely on any single control for authorizing high risk transactions, but rather institute a system of layered security,” the guidance states.

Gartner’s Litan says non-banking entities should take a page from U.S. financial institutions and embrace the layered security approach.

“Fraud is advanced in financial services, because that’s where the money is,” Litan says. “Other sectors are many years behind banking and financial services, when it comes to fraud prevention and are generally not even thinking about a layered security approach.”

But fraud is migrating, and in some cases, the techniques and attacks waged in other sectors are just as sophisticated as the ones launched against financial services. “The response of these non-financial organizations should, similarly, be advanced,” Litan says.

3. Customer Awareness

Security leaders universally acknowledge that people are their weakest link. And organizations routinely pledge to do a better job of security awareness with employees and customers alike.

The FFIEC Authentication Guidance takes this acknowledgement a step further and prescribes minimum standards for banks’ awareness programs. Going forward, U.S. financial institutions must develop customer awareness and educational efforts that include:

- An explanation of protections provided, and not provided, if and when an online breach occurs;
- An explanation of when and how a customer could be contacted by the institution for information about electronic banking credentials;
- Suggestion that customers perform their own periodic risk assessments;
- A listing of alternative risk control mechanisms customers may consider to mitigate their own risks, and/or a listing of resources where such information can be found;
- A listing of institutional contacts customers can call if suspicious activity is picked up.

The objectives are to raise customer awareness to the threat landscape, as well as to minimize customer susceptibility to common social engineering schemes such as phishing.

Again, these goals translate well across all sectors, but the FFIEC is at the forefront of the movement, Litan says.

“I don’t see commensurate programs in other industries,” she says. “It’s important to make your customers and employees aware of potential fraud that can occur against them. They need to participate in the solution – and not just in the problem.” ■

Tracy Kitten is Managing Editor of BankInfoSecurity.

the FFIEC says that institutions’ layered security programs must include two elements:

- Anomaly Detection - processes designed to detect anomalies and effectively respond to suspicious or anomalous activity;
- Control of Administrative Functions - enhanced controls for system administrators who are granted privileges to set up or change system configurations, such as setting access privileges and application configurations and/or limitations.

Further, the guidance goes on to recommend nine specific security controls that may be part of a layered security program. These controls include (but are not limited to):

- Fraud detection and monitoring systems that account for customer history and behavior, and enable timely and effective responses;
- Dual customer authorization through different access devices;
- Out-of-band verification;
- “Positive pay,” debit blocks or other techniques that limit transaction amounts;
- Enhanced controls over account activities, such as transaction value thresholds, payment recipients, number of transactions allowed per day and allowable payment windows, such as specific days and times;
- Internet protocol reputation-based tools to block IP addresses known or suspected to be associated with fraudulent activities;
- Policies for addressing customer devices that have been compromised and may be facilitating fraud;
- Enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels;
- Enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk.

Automation with a Dash of Humanity

Experts Focus on Components of a Continuous Monitoring Program

By Eric Chabrow

As organizations move to the continuous monitoring of their IT systems to assure they're secure, governments, businesses and not-for-profits rely much more on automated processes.

"The attacks are coming at automated speed over the Internet and the attackers have many more people than we have to defend, so in the kind of environment that I sit in, it would be impossible to do it without automation," says George Moore, chief computer scientist at the U.S. Department of State, in a roundtable discussion on information risk management.

Automated tools help organizations identify information assets that need to be monitored. "So many breaches occur because people didn't know data was even located in the area where the incident occurred to begin with," says IT security and privacy consultant Rebecca Herold.

But don't forget the role people play.

"Certainly, we can't do this job of continuous monitoring without automation," says NIST Senior Computer Scientist Ron Ross. Automation "is a necessary piece, but not sufficient, because there are a lot of things that only humans can do and humans do best."

Processes to continuously monitor insider threats require human intervention. "The combination of these activities really will work well to do what we would call a very robust continuous monitoring program," Ross says.

The panel features Ross, who leads the National Institute of Standards and Technology's information risk management framework guidance initiatives; Moore, who helped shepherd State's global continuous monitoring program; Herold of Rebecca Herold and Associates, who advises healthcare organizations; and John Carlson, BITS executive vice president, who oversees the financial

services roundtable's cybersecurity and fraud prevention initiatives.

What follows is an edited excerpt of the panel's discussion on automation moderated by Information Security Media Group Executive Editor Eric Chabrow.

ERIC CHABROW: As we look at organizations today, there are more stakeholders, there are more threats, there's a lot of complexity here. Can proper information risk management be done without automation?



"There are a lot of things that only humans can do and humans do best."

- RON ROSS, NIST

GEORGE MOORE: I would say not. The attacks are coming at automated speed over the Internet and the attackers have many more people than we have to defend. In the kind of environment that I sit in, it would be impossible to do it without automation.



REBECCA HEROLD: Automation is necessary in many different ways. One of the things that I've seen over the years is that organizations don't even know where their data is located. How are you going to know how to protect that data if you don't even know where it resides? One type of automation that I've found

Continuous monitoring cannot succeed without the vital contributions of individuals.

is very helpful are these tools now that you can use to identify where your data is located – your critical data, your protected health information or any other types of sensitive information – and then keep an inventory of that up-to-date using automation. That way, you'll know where this data is at and how the risk levels are based upon its location. So many breaches occur because people didn't know data was even located in the area where the incident occurred to begin with.



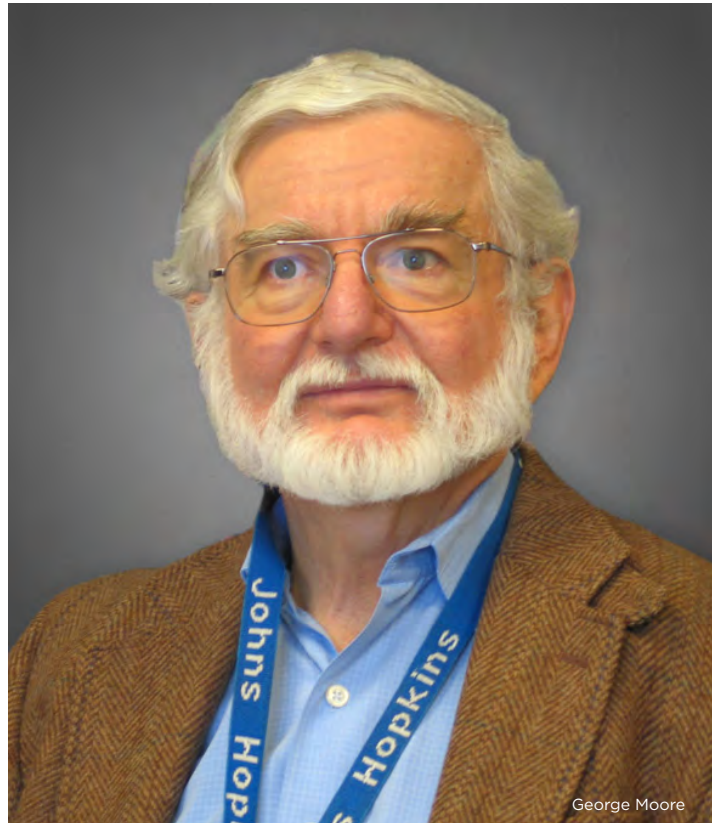
John Carlson

JOHN CARLSON: In addition to the automation point, which I agree with, is that you do need to still have forums for experts to talk to one another about the changing threat environment. That's one thing that I think the financial services community has done a very good job dating back 12 to 13 years ago and establishing an information sharing and analysis center on ISAC for experts to get together and talk about the changing threat environment and tactics for how to respond.

It has also provided forums to have discussions with government officials around the changing threat environment and how we can work together in partnership with the appropriate controls in place to protect the information or to not subvert, say for example, a law enforcement investigation that may also be going on concurrently. [That way,] we can protect the industry and the sector and the economy from any sort of large-scale cyberattack or malware attack that could affect multiple institutions. It's a combination of good, strong controls with automation at individual institutions, but also a way to collaborate across the industry, and where necessary, with government agencies and with other sectors, since many times, we're all using the same operating system or the same suppliers across multiple sectors. We have to recognize that it's a combination and it really has to be a collaboration and a partnership.

RON ROSS: I would agree with everybody who's said it's a combination. Certainly, we can't do this job of continuous monitoring without automation. It's certainly a necessary capability, but not sufficient.

If you look around, there are a lot of things that automation can do that humans don't do very well, and certainly the inventory management and also something I know George has been very much involved in is the automated checking of configuration settings that ... some are part of the SCAP (Security Content Automation Protocol) program that NIST runs, so you have these



George Moore

“The attacks are coming at automated speed over the Internet and the attackers have many more people than we have to defend.”

- GEORGE MOORE, CHIEF COMPUTER SCIENTIST, U.S. DEPT. OF STATE

configuration settings that are established on laptop computers, portable devices, that actually eliminated attack factors that adversaries may use to compromise your systems. Ultimately, it's a necessary piece, but not sufficient, because there are a lot of things that only humans can do and humans do best, and certainly, when you talk about the insider threat and being able to monitor certainly bad actors or people whose privileges should be reduced because of certain types of activities.

There's a whole series of things in the management and operational space which are also very much amenable to continuous monitoring, not with automation on a regular basis as determined by the organization, but I think the combination of these activities really will work well to do what we would call a very robust continuous monitoring program. ■

To hear the entire roundtable discussion, please go to:
<http://www.govinfosecurity.com/interviews.php?interviewID=1325>

The State of Security Education

Purdue's Spafford Says 'We're Still Playing Catch-up'

By Tom Field

Information security threats – especially to critical infrastructures and from nation-states – are evolving. But security education curricula are struggling to keep pace, according to Eugene Spafford, renowned information security professor at Purdue University.

“We’re still playing catch-up, I think, in the educational environment,” says Spafford, discussing the current state of information security education. “The majority of places where we are teaching information security concepts, secure programming and some of the other issues are still being done by faculty who have limited exposure in the area. And they’re having to use existing educational materials, many of which were developed in years past, before many of these issues were well understood.”

But more than just the educators and institutions, students also need to change their traditional approach to education. Training isn’t enough, Spafford says. It’s time for information security students to focus on being true professionals.

“The real value, the real chance to make a difference is by treating [information security] as a profession,” Spafford says. “Training will get you a job. Education – especially ongoing education – is part of being a professional. And that’s where I think the future really lies for many people in this field.”

In an exclusive interview on the state of security education, Spafford discusses how today’s students need to evolve to fill tomorrow’s jobs.

Spafford is a professor with an appointment in Computer Science at Purdue University, where he has served on the faculty since 1987. Spafford’s current research interests are primarily in the areas of information security, computer crime investigation and information ethics. He is generally recognized as one of the senior leaders in the field of computing.

FIELD: How do you see information security jobs evolving?

SPAFFORD: The kinds of positions that students are going into are becoming increasingly specialized. Incident response, investigation, architecture and operations are four areas that are certainly becoming distinct. We’re also seeing an increasing interest in individuals who understand the privacy aspects of security, and that may also become somewhat of a specialization area. All of this is because there’s simply too much material really to pack into one degree program if we’re looking at a higher-education environment in its current form.

There are so many different problems and circumstances that generally



Eugene Spafford

“There’s a real commitment here to be a professional rather than simply a student.”

- EUGENE SPAFFORD, PURDUE UNIVERSITY

students are able to pick an area and focus on it, or else they get a very general education that’s going to require additional training afterward. The market is very strong. Pretty much anybody who gets a good grounding in any of these areas from a regular institution is going to have no difficulty finding employment, assuming that they’re willing to relocate. But at the same time, we simply don’t have the resources to produce all the students and all the graduates who are necessary to fill all of these areas.

FIELD: How do students have to step up and play new, more-advanced roles?

SPAFFORD: They're going to have to spend a little more time with hands-on learning in some cases than perhaps has been the case at some institutions, because actually being able to operate some of the technology is going to be important. But more importantly I think is something that hasn't been a case for perhaps a decade or so. We're going to have to develop more of a cultural way of learning and more than simply studying for tests, cramming for tests or doing projects while in classes. These students are going to have to get into the habit of reading the news, reading the industry news and being prepared to go to conferences or training sessions to continue to hone their skills. The field is advancing rapidly. We can't teach it all in a higher-education setting, and so anyone who's going to work in this field must become a life-long student and be very focused on that rather than simply putting in 9-5 or 9-8 or whatever hours they have and then kicking back for the rest of the day. There's a real commitment here to be a professional rather than simply a student.

FIELD: For somebody wanting to enter the information security profession in 2012, what would you sit down and offer them for advice?

SPAFFORD: I would suggest to them to think of two paths here. One is they could certainly get a job in the area where they are effectively a technician, where they go to work, do some things and then go home. But the real value chance for advancement and chance to make a difference is in treating this really as a

“Training will get you a job. Education – especially ongoing education – is part of being a professional.”

- EUGENE SPAFFORD, PURDUE UNIVERSITY

profession and that gets to my earlier answer. It's very similar to what one might encounter in becoming a doctor, lawyer or college professor, where you have to devote yourself to life-long education and development and continuing to hone your skills. Part of being a professional is to actually continue to improve in what you're doing, rather than treating it simply as a job. I have made a distinction in the past in talking with you between training and education. I think it's time to also make the distinction between having a job and being part of a profession. ■

To hear the entire interview, please go to:

<http://www.careersinfosecurity.com/interviews.php?interviewID=1300>

Managing security systems at the new World Trade Center is more than a challenge. It's an honor.

**BOLD
SECURITY
CHANGES
ALL.**

Diebold's security integration connects an array of systems, giving operators unified control and citizens peace of mind. It's another example of Diebold doing more to build relationships. Relationships that have inspired us to become leaders and innovators in the security industry for more than 150 years.

For more information, e-mail us at security@diebold.com
or visit us at Booth #757 at RSA.

DIEBOLD
INNOVATION DELIVERED®

Come Join Us at Our Sessions...

ISMG Hosts Two Timely Presentations at RSA Conference 2012

SESSION 1:

How to Launch a Secure Cloud Initiative: NASA's Jet Propulsion Laboratory

Wednesday, February 29, 10:40 AM
Room 305

Organizations in all sectors embrace the efficiencies and cost-savings of cloud computing. But they're frequently challenged by the task of ensuring data security and privacy in the cloud. This session offers exclusive new research findings on cloud computing, including a case study of NASA's Jet Propulsion Laboratory and how it launched a successful, secure cloud computing initiative.



Session attendees will gain insights to help them:

- Compare the benefits of various types of cloud offerings
- Evaluate their own cloud readiness levels on a numeric scale
- Negotiate better cloud computing contracts with vendors
- Measure their own success

Presented by



Eric Chabrow

Executive Editor, Information Security Media Group

Eric Chabrow oversees InfoRiskToday and GovInfoSecurity. A veteran journalist who has covered IT, government and business, Chabrow is the former top editor at the award-winning business journal CIO Insight and a long-time editor and writer at InformationWeek. He was on the team that developed Time Inc.'s teletext venture, a precursor to today's Internet website.



Tomas Soderstrom

Chief Technology Officer, NASA JPL

Tomas Soderstrom serves as the IT Chief Technology Officer at NASA's Jet Propulsion Laboratory, where his mission is to identify and infuse new IT technologies into JPL's environment. Soderstrom has led collaboration product developments, and has been a consumer of collaboration techniques and tools.

SESSION 2:

The Faces of Fraud: An Inside Look at the Fraudsters and Their Schemes

Friday, March 2, 9:00 AM
Room 102

From remote pockets of the world, they strike - organized rings that target ATMs, point-of-sale devices, payment cards and bank accounts. Today's fraudsters are sophisticated, organized and persistent. This session offers the U.S. Secret Service's inside look at exactly who these fraudsters are, as well as BankInfoSecurity's newest study of today's hottest fraud schemes - and how to stop them.



Participants will gain insights to help them:

- Recognize the most common forms of fraud facing financial institutions
- Understand the mindset of today's fraudsters
- Deploy the latest, most effective technology solutions
- Bridge the organizational silos that inhibit cross-channel fraud detection

Presented by



Tom Field

Editorial Director, Information Security Media Group

Tom Field is an award-winning journalist with over 20 years experience in newspapers, magazines, books, events and electronic media. A veteran community journalist with extensive business/technology and international reporting experience, Field has written news, sports, features, fiction and analysis for publications ranging from Editor & Publisher to Yankee Magazine.



Erik Rasmussen

Special Agent, US Secret Service

Erik Rasmussen has been a Special Agent with the United States Secret Service ("USSS") since August 2004. He is currently assigned to the Criminal Investigative Division, Cyber Intelligence Section. Prior to this assignment, he worked on the Electronic Crimes Task Forces for the Los Angeles and Seattle Field Offices.

PANEL WEBINAR

MOBILE TECHNOLOGY: HOW TO MITIGATE THE RISKS



SMART PHONES, LAPTOPS, TABLET PCS,
OPTICAL DISCS AND USB DEVICES.

There are many new mobile devices and emerging technologies to help today's professionals do their jobs in any location - and increasingly private business is being conducted on personal digital and storage devices. How do you ensure that critical information remains secure on personal mobile devices - even when the devices are lost or stolen?

Presented by a panel of experts



Terrell Herzig
CISO, UAB Medicine



Paula Skokowski
VP - Products &
Marketing, Accellion



Scott Ashdown
Director - Products
& Solutions, Imation



Robert Hamilton
Senior Product Marketing
Manager - Data Loss
Prevention, Symantec

Learn More

Visit BankInfoSecurity.com/mobile-panel

When it comes to

We've got you covered.

News | Education | Research



Complete coverage of RSA® Conference 2012. News, interviews, and analysis right from the conference floor. Scan the QR code with your smartphone to see all our coverage.

