CyberCrime
2011 Symposium

# Security in the Age of WikiLeaks – Cybercrime, Espionage and Hacktivism

**November 3-4, 2011**

## Conference Insights

# Table of Contents



# Conference Insights

Building on the momentum of its 2010 debut event, Sage Data Security presented its CyberCrime 2011 Symposium to a packed house of attendees from the financial, healthcare, and government sectors. The symposium featured two days of interactive presentations by cybercrime experts from both the public and private sectors, including journalists, federal law enforcement, malware researchers, C-level security officers, forensics analysts, attorneys, public relations professionals, and cyber-bullying prevention educators.

**"Security in the Age of WikiLeaks — Cybercrime, Espionage and Hacktivism"** explored the global cybercrime epidemic within the context of the WikiLeaks phenomenon. Attendees were treated to discussions surrounding every aspect of the fast-evolving cybercrime ecosystem — from its players, arsenal of tools, and targets, to its emboldened attitude, financial and political motivations, and 'achievements' — and received a range of recommendations for defending their organizations against network attacks. They also participated in an incident response exercise simulating an attack on a municipal government that tested their security breach analysis and reaction skills in real-time.

## Conference presenters:

**Kevin Poulsen**, **Senior Editor, Wired.com:** *"WikiLeaks – Is Any Secret Safe?"*

**Jerry Gamblin, Security Specialist, Missouri House of Representatives**: *"50 Days of Mayhem: What We Can (and Should) Learn from LulzSec"*

**Joe Stewart**, **Director of Malware Research, Dell SecureWorks:** *"The Malware Behind the RSA Breach and other Advanced Persistent Threats"*

**Matthew O'Neill**, **Special Agent, United States Secret Service:** "*Investigating Cybercrime"*

**Brian Krebs**, **Editor, Krebsonsecurity.com:** *"ZeuS, Thieves, and Money Mules"*

**Dave Ostertag**, **Global Investigation Manager for Incident Response, Verizon Business Solutions:** *"Learn from the Mistakes of Others: Be Better Prepared to Combat Security Risks to Your Organization — Insights from the 2011 Verizon Data Breach Investigations Report"*

## Team Session, "What You Need to Know Before It Happens to You"

**Benjamin Greenfield**, **Security Engineer, Google, Inc.:** *"Forensics Fundamentals"*

**Peter Guffin, Attorney, Pierce Atwood:** *"46 States and Counting: State and Federal Notification Requirements"*

**Ross Levanto, VP, Schwartz Communications:** *"Public Relations Rapid Response"*

**Scott Godes**, **Attorney, Dickstein Shapiro Cyber-Insurance Practice Group:** *"Cyber-Insurance: Will You Be Covered if Your Company Suffers a Cyber-Event?"*

**Phil Fogelman**, **Director, New England Region, World of Difference Institute:** *"Making the Internet a Safer Place for our Children and our Community"*

In these presentations, speakers diagrammed 2010-2011's astounding contribution to the annals of cybercrime, characterized by conference host Sari Greene as "an incredible year of data compromise and exposure." The period started with the insider leak of a massive amount of classified data that was published by WikiLeaks, and included high-profile breaches at Epsilon, RSA, and Sony, LulzSec's 50-day reign of "entertainment," escalating state-sponsored espionage activity, and a growing number of corporate account takeover attacks and additional breaches targeting financial, healthcare, government, and other sectors.

This Cybercrime 2011 Symposium Insight details the conference's key takeaways, outlining the primary challenges facing organizations as well as recommendations for recognizing, responding to, defending against, and recovering from cybercrime, espionage, and hacktivism.

## Takeaways

- No electronic data is safe from the human element.
- Financial gain is a primary motivator behind hacks. Increasingly, so are politics, payback, harassment, and "entertainment."
- While some attacks are extremely sophisticated in nature, they don't need to be — many succeed through straightforward, unrelenting persistence.
- Cybercriminals and other hackers are the biggest threat to security, but employees do their share.
- Federal law enforcement assigned to cybercrime is understaffed relative to the enormity of the threat, but agencies are making headway.
- If you're breached, suck it up. Notify authorities, perform forensics analysis, assemble your PR team, and contact your insurance providers.
- Community outreach programs raise awareness of the impact of cyber-bullying by educating school administrators, parents, children, and the larger community.
- Get serious about a strategic security awareness program that treats every member of your organization as a core member of the security team.

## Takeaway: No electronic data is safe from the human element.

**What would you do if you had access to classified networks for 14 hours a day, seven days a week, for eight-plus months?**

The question Army intelligence analyst Bradley Manning asked hacker Adrian Lamo during one of their early online chat sessions — the transcripts of which would later link Manning to WikiLeaks — holds chilling significance given everything that came after. It's a question every IT security professional within every public and private sector organization needs to consider in intimate detail when developing security policy. Individual responses to the question are, of course, innumerable, making the underlying message singularly clear: No electronic data should be considered safe from the human element.

Manning would eventually answer his own question with the leaks of hundreds of thousands of classified documents — Iraq and Afghanistan war logs, State department diplomatic cables, and video of a 2007 Apache helicopter airstrike in Iraq that killed a journalist and other civilians. According to his own statements in the chats with Lamo, Manning was motivated by his conviction that what he'd seen in diplomatic cables and army databases highlighted U.S. wrongdoing, and further encouraged by his belief that someone with access to NSA databases must have leaked the half-million-plus 9/11 pager messages that WikiLeaks published in 2009.

Motivation met motivation when Manning submitted to WikiLeaks the Apache airstrike video, which the organization published in April 2010. From the outset, WikiLeaks founder Julian Assange, according to speaker Kevin Poulsen — a journalist who would play a leading role in the Manning/WikiLeaks narrative — "created an environment where nothing could be counted on to be kept secret." In words and action, said Poulsen, Assange broadcast his worldview that "governments, at their worst, operate as conspiracies, and to function they need the ability to keep secrets within the conspiracy. If they can't trust everyone within the conspiracy it becomes dysfunctional and dissolves."

Enabling Assange's mission of exposing corruption and conspiracy is a global technology infrastructure that allowed WikiLeaks to distribute sensitive material with a breadth and depth heretofore unimagined. Digital video, CSV files, and entire databases met the government's Secret Internet Protocol Router Network, which in turn met a secure leak submission system hosted by an organization whose reason for existence was "open diplomacy." When the goal of cyber-espionage is exposure, entire databases of information can be disseminated to a worldwide audience with a simple click. Beyond that, this content can be indexed in a searchable format to ensure no detail escapes notice.

Prior to the arrival of Manning on the scene, WikiLeaks had posted around 20,000 mostly obscure documents, with a few significant exceptions. The release of Manning's video, entitled "*Collateral Murder*" by WikiLeaks, catapulted the organization and Assange onto the world stage in 2010. The publicity the video generated may have encouraged Manning to go further. He went on to submit the Afghanistan war logs, Iraq war logs, and more than 250,000 U.S. State Department diplomatic cables to WikiLeaks.

Logs of the chat sessions with Lamo revealed details on Manning's motives for the leaks, his sense of isolation in Iraq, problems adjusting to military life, his gender identity confusion, and his distress over "the loss of all his emotional support channels." Based on his own fears that what Manning was doing would put lives in jeopardy, Lamo showed the logs to the FBI, which immediately moved to have Manning arrested. Manning is now in pretrial custody in Fort Leavenworth, Kansas; his Article 32 hearing started just over a month after the symposium. He is charged with several crimes, including the capital offense of aiding the enemy.

An overarching lesson from the WikiLeaks fallout is that no amount of technological armament can protect an organization from the human component. Political ideology, ego, fear, emotional instability, personal and professional pursuits, and countless other emotional drivers were at work. Technology provides the tools to secure an infrastructure, but only to the extent that people allow: Security professionals have to factor in all the human elements both inside and outside their firewalls if they hope to secure their organizations' digital assets.

**Takeaway: Financial gain is a primary motivator behind hacks. Increasingly, so are politics, payback, harassment, and "entertainment."**

Hacking continues to be largely financially motivated, but as networks connect world populations as never before, state-sponsored political espionage and a more recent arrival, "hacktivism," likewise contribute significantly to breach activity.

"In the past, hacking for civil disobedience was practiced by people who were typically willing to go to jail for something," said Poulsen. "What perpetrators are calling 'hacktivism' now looks like digital thuggery with a political motive tacked on."

From the standpoint of security officers charged with protecting an organization, it doesn't matter whether cyber-espionage reveals the actions of oppressive regimes, or takes civil disobedience to new levels, or merely seeks to publicly embarrass an individual. Because technology has made it so easy for even marginally talented hackers to breach defenses, the security seat is the hot seat, requiring extreme vigilance.

> **"What perpetrators are calling 'hacktivism' looks like digital thuggery with a political motive tacked on."**
>
> **– Kevin Poulsen, Wired.com**

Highlighting the new breed of hackers in 2011 was LulzSec's 50-day reign of 'entertainment.' The group, interchangeable with the Anonymous and Anti-Sec movements, pulled off several high-profile attacks during the year, targeting individual and corporate reputations and wallets. The list of victims included a who's who of large corporations as well as much smaller targets, all carried out by a small team of tech jocks.

Amazon, PayPal, Sony, and numerous other organizations were targeted for varying reasons and to varying results, but in some cases the damage was extensive. LulzSec/Anonymous took down Sony's Playstation 3 network for three weeks, stealing 70 million records and another 25 million from Sony Online Entertainment, causing reputational and fiscal damage, according to presenter Jerry Gamblin. Some companies, including PayPal and Amazon, were targeted as a direct result of actions they took in response to the WikiLeaks situation, while others were victimized simply because they caught the attention of LulzSec members.

Arrests that began with Jake Davis — code-named "Topiary" and considered the brains behind the hacks — and continued with other members, revealed that the average group member was a young male. This included 19-year-old Ryan Cleary, or TFlow, who was running the LulzSec server from his parents' house. LulzSec's reign shifted the hacker profile yet again: the public's early perception of the typical hacker as a teenager with a vendetta, which had evolved in recent years to view hackers as cogs in organized global crime syndicates, once again included the teenager with a vendetta.

"We do a disservice when we say not to worry anymore about the 18-year-old in the basement because in many cases, these are the guys coming after you first," said Gamblin. These hackers are intelligent and technically adept, but they don't need to be criminal geniuses or be using advanced security-cracking tools to get into an organization. Tenacity and drive, coupled with some relatively basic platforms and tools, have allowed them to be very successful in their efforts. "They're not out there using super-advanced hacking techniques or breaking new ground; they're using what's readily available," Gamblin said.

Anonymous members "love to proclaim what they've done loudly" through Twitter posts, said Gamblin, as well as to engage in public battles with anti-anon "vigilantes." All this virtual crowing and high-fiving serves a larger, darker hacker community need, he said. "If you're a hacker that's part of an organized crime syndicate that's working to be profitable and hacktivists are attacking sites and trumpeting their successes, you just let them keep doing it and keep your head low." They provide a smokescreen that lets syndicates continue to build their criminal network while someone else takes the glory, the press — and the heat.

**Gamblin's bottom line:** If you can't defend against the proverbial "18-year-old in the basement," you have no chance defending against the groups engaged in corporate espionage or state-sponsored activity.

**Takeaway: Though some attacks are extremely sophisticated in nature, they don't need to be – many succeed through simple unrelenting persistence.**

The prolific work of **Anonymous and LulzSec** highlights the damage that can be done using basic tools and techniques, as well as weakens the hacker community stance that real hackers don't use simple tools. "There's a continuing view among hackers that you're not a real hacker if you're using point-and-click tools, but the bottom line is people are getting hacked by attackers using these tools," says Gamblin. "There are still very talented guys out there who can write Perl and Python script and really own you, but that's primarily when the motive is monetary gain."

> **"There's a continuing view among hackers that you're not a real hacker if you're using point-and-click tools, but the bottom line is people are getting hacked by attackers using these tools."**
>
> **– Jerry Gamblin, Missouri House of Representatives**

Tool simplicity is sometimes the modus operandi of even the type of "advanced persistent threats" (APTs) used in cyber-espionage activity targeting government or industry secrets, said presenter **Joe Stewart of Dell SecureWorks**. Stewart and his Counter Threat Unit (CTU), through an analysis effort to classify families of custom malware used for cyber-espionage, traced the 2011 RSA breach to an attack originating in China.

"The APT in this realm is like the LulzSec techniques — it's more about the 'persistent' than it is about the 'advanced,'" said Stewart. "A lot of the trojans we've examined aren't that advanced and don't have to be. This threat is more about actors getting into networks and maintaining their hold there so they can suck out as much data as they can."

APTs gained ground in the early 2000s when they primarily targeted government military contractors, but lately, they've expanded significantly to target a range of industries — some expected and some "very surprising," according to Stewart. Examples he cited:

- **Google.** When Google was targeted in Operation Aurora, observers were perplexed as to why China would want to target Google secrets as part of their cyber-espionage strategy. They didn't — they wanted the email accounts of Chinese activists and rather than hack into accounts individually, they wanted access to Google's back-end email servers to get the whole smash.
- **Software vendors.** APT actors use zero day exploits, and rather than do in-depth research on numerous potential targets, Stewart theorizes, they may hit software vendors because of their broad customer base. If they can obtain source code or vulnerabilities at this level, they can develop zero day exploits for the vendor's software instead of conducting blackhawk research on individual organizations.
- **Activist organizations.** These groups are ongoing targets, especially for APT actors in China trying to root out anti-communist activist groups.

- **Manufacturers.** High-tech manufacturers, particularly, are targets.

- **Law firms.** Companies specializing in patent law have databases with reams of intellectual property information; to capture that can be a huge differentiator to competitors engaged in industrial cyber-espionage.

One of the more high-profile APT actors is the "Comment Crew," so named because they like to hide commands in html comments, said Stewart. Basically, they use spear-phishing to install a small downloader trojan on an organization's web site that periodically requests a web page with additional instructions using the typical stage-one phone-home process. Then, they use this first-stage trojan to deliver the payload by pulling a large piece of malware with full shell capabilities, tunneling, and other advanced features.

In its report on the Comment Crew's well-documented Operation Shady RAT, McAfee identified 72 targets across a range of industry and government sectors. Targets included military, construction, electronics, computer security, communications, energy, news media, and agriculture sectors. Further analysis by CTU revealed 15 additional victims, including more defense contractors, an Asian nation's Air force, a financial news service, a global policy expert, and a biomedical institute.

The key takeaway from Shady RAT, said Stewart, is that while it might seem to have victimized a large number of companies and sectors, the operation represents just the tip of the iceberg. Said Stewart, "Victimizing this number of organizations is nothing. These guys have much more infrastructure, have deployed many more trojans, and have access to a crazy amount of data." Comment Crew has at least a dozen variants of malware that behave similarly to Shady RAT and many more second-stage backdoor trojans, each with several known control servers. CTU has tied more than 100 different control servers to Comment Crew, but Stewart believes the number is much larger given the number of trojans the group has deployed.

Further, Comment Crew is one of two major actor groups, with several minor groups also at work. The groups work in sync, assigning multiple coders on multiple teams to develop trojans to exfiltrate as much data as possible, or use trojan source code they purchase and then customize. Their intent, said Stewart, Is extensive coverage so they ensure something gets through defenses. They use zero days when they have them, but they're also happy to use old exploit techniques because they still tend to work, especially on targets that don't keep up with third-party software patches and other updates.

Through traffic behavior analysis in its RSA classification exercise and ongoing research, Stewart's team also determined that Comment Crew and its counterparts use HTran, a packet bouncer/relay that disguises the true location of command and control malware servers. HTran, however, can betray the location of a control server; when it loses connectivity with a back-end server, an error message goes to the connecting client and provides insight into APT activity not otherwise seen.

Based on analysis of thousands of host names, CTU developed a map of IP address locations, which point primarily to Beijing, Shanghai, and Hong Kong. This attribution goes beyond regular IP-based attribution, but "It only proves the 'where' and not the 'who,'" said Stewart. "We might know all this is state-sponsored activity but we can't prove it's the PLA [People's Liberation Army] without digital evidence. Still, it's getting harder for them to deny they're involved."

Beyond "complaining about the problem at State Department meetings," Stewart said organizations should deploy their own "defense-in-depth" strategies to defend against malicious attacks that rely on numerous exploits.

## Takeaway: Cybercriminals and other hackers are the biggest threat to security, but employees do their share.

**External threats to organizational data are large in both type and number of attackers. But what about threats that come from inside your organization?**

Brian Manning is only the most famous case of an insider threatening data security. Internal actors, including corporate executives, lower-level employees, and independent contractors, are significant contributors to data breaches in organizations worldwide, whether maliciously or through simple error.

In his presentation highlighting findings from Verizon's 2011 Data Breach Investigations Report — which represents the combined findings of Verizon, the U.S. Secret Service, and the NHTCU gleaned from cases where data is exfiltrated — David Ostertag revealed that 17% of breaches in 2010 were caused or aided by insider activity. While this figure is down significantly from 2009's 48%, Ostertag believes this percentage decline is largely a function of the huge increase in the number of external attacks in 2010 than it is an actual decrease in internally caused compromises.

Understandably, many security leaders are surprised when they find out an employee caused a security breach. "The first question they ask when they're told about an internal breach is 'Was it intentional?'" said Ostertag. In 2010, in fact, 93% of internal data delivery breaches were deliberate and malicious, according to report findings.

In 2010, breaches caused by employees nearly always involved using privileges or resources in ways other than those dictated by policy. According to the 2011 report, 79% of misuse cases involved highly malicious acts such as embezzlement and card skimming. Nearly half (49%) involved the abuse of system privileges/access, while 39% was related to the use of unapproved hardware and devices. Less-frequent misuse scenarios included violating web (5%) and email/IM policies (4%). Very few cases of data compromise are the result of simple error, which include improper data disposal, inadvertent publishing of data, programming mistakes, or errors of omission, such as neglecting to change default access credentials.

> **"When an employee has multiple policy violations, we see a direct correlation to internal data breaches."**
>
> **– David Ostertag, Verizon Business Solutions**

While there are numerous high-tech methods employed by privileged users to steal funds and exfiltrate data, common perpetrators of less-complicated forms of embezzlement include retail employees, wait staff, bank tellers, and others whose jobs involve financial transactions. With physical breaches, there's an increasing use of skimmers and other devices to conduct theft.

In the case of both intentional and unintentional misuse of electronic privileges and resources, security professionals usually have warning signs. "When an employee has multiple policy violations, we see a direct correlation to internal data breaches," said Ostertag. "Often, there's something happening outside the office environment — a divorce, health problems, a bankruptcy — at the time a breach occurs." An employee violates policies frequently either because they've decided they're going to steal from the organization, or because they've gotten sloppy in their work, creating a hospitable environment for a data breach. If security professionals see a series of policy violations, they should intervene.

**Takeaway: If you're breached, suck it up. Notify appropriate authorities, perform forensics analysis, assemble your PR team, and contact your insurance providers.**

## Who Needs to Know?

So you've been breached. After you suppress your panic, it's time to work your breach plan. That includes notifying appropriate parties, assembling the PR team, contacting your insurance providers, and when necessary, performing forensics to confirm breach activity.

It's tempting to keep a data breach secret, but not reasonable. To date, 46 states and the federal government have statutes addressing notification for data breaches, backed up by fines for violations and thresholds for notifying the media. In most states with notification regulations, said Peter Guffin, an organization needs to notify authorities and victims if a breach involves "unauthorized acquisition, use, or access to personal information that threatens the integrity or security of that information, creating a risk of identity theft." Currently, statutes cover just "personal information" (PI) accessed in a breach and not larger business-owned targets like intellectual property.

Companies with US headquarters doing business worldwide not only have to deal with state and federal regulations, but foreign regulations as well. But even for a company just doing business in the U.S., breach notification compliance is complex, considering that state statutes vary and federal regulations typically take precedence. Determining your obligation to constituents as it relates to PI compromise requires that you understand what was compromised, whose PI was involved, what law enforcement to notify, where affected parties reside, and whether there's actual harm. Throw in federal regulations like Gramm-Leach-Bliley, HIPPA, and the HITECH Act, and dealing with the after-effects of breaches can be as involved as thwarting them.

> **"Disk space is inexpensive and some incredible tools are available, so not capturing logs is negligent."**
>
> **– Ben Greenfield, Google**

The theft of encrypted data, for example, doesn't constitute a breach in many cases, as long as the encryption key isn't compromised. Under the HITECH Act, only unsecured PHI (protected health information) is considered; PHI data that's encrypted to standards or "de-identifed" isn't subject to penalties or notification requirements.

Because failure to comply with breach regulations can result in fines, reputation damage, and lost customers, your organization should have a plan in place for handling PI compromises. Guffin's advice: centralize breach management activities and processes, and if breached, do triage based on affected individuals' states of residence and applicable federal guidelines.

## What Happened?

You're seeing suspicious activity on your CFO's workstation and suspecting a breach. Now you need to confirm your suspicions. Some organizations turn to forensics analysis to determine if a breach actually occurred, and if it did, the relevant details. Analysis can uncover "indicators of compromise" that enable you to effectively search your entire network for more indicators, "intrusion sets" that reveal specific actions behind an attack, and the level of "common vulnerability exposure" involved. Beyond these findings, you want answers to higher-level, business-critical questions: Was customer data compromised? Was it exfiltrated? How extensive was the damage? Do you need to notify people?

However, said presenter Ben Greenfield, "digital forensics is not some magical place where you get the answer to all your questions — it's the process that takes place because something bad happened to something electronic on your network." The classic workflow of a forensics investigation, which involves offline analysis — often of a single end-point device — is highly technical and isn't set up to answer these larger questions.

Nonetheless, digital forensics is an instrumental tool for confirming breaches and providing critical technical details. However, its ultimate value varies significantly based on the evidence you provide analysts following a breach. In a classic workflow, events unfold like this: A technician sees something suspicious on a workstation, and, as taught, immediately pulls the plug on the machine to preserve evidence. This step is important because digital forensics rely on a device's image at the time a problem manifests, allowing an analyst to work back from that point. Then the tech physically confiscates the evidence, starts chain-of-custody documentation, and hands it off to incident responders. Forensics analysts capture the machine's unique hash, create a full image of the drive, update the chain of custody forms, and put the original drive in a fireproof safe. Only then do they mount the work copy and start their analysis.

If the hard drive holds the only evidence of a breach you can provide, you've severely limited the information digital forensics can deliver. Forensics can reconstruct the events of the breach, but with just end-point evidence, it's difficult to determine what technology and policy changes might prevent similar breaches. Further, chain-of-custody and imaging processes eat up 24-48 hours before analysis can even begin.

The less information you can forensics analysts, the lower the baseline starting point and the more they'll have to figure out on their own. The good news, said Greenfield, is that "it's inexpensive to avoid putting yourself in this position. Breaches are really expensive but disk space is really cheap, so keep the logs for networks and devices so you have visibility into data access and other activities." By storing logs, you can provide analysts with archived data to compare against evidence.

To facilitate processes that reveal useful information in the event of a breach, you need an incident preparedness plan. To accomplish this, round up all your logs and determine which will help you improve incident response and store them going forward. "Disk space is inexpensive and some incredible tools are available, so not capturing logs is negligent," said Greenfield.

A forensics analyst will ask for the logs for browsers, firewalls, internal switches, and other network devices. "If you give them one hard drive, they'll be forced to come back to you with lots of questions," said Greenfield. "But if you can give them a full network-capture of everything that occurred on the network in the last 30 days, they'll be coming back to you with lots of answers," said Greenfield.

## Time to Tell the Tale

Some states have thresholds in place that dictate when a breached company needs to contact the media, but in the absence of those, it's still a good business practice to conduct outreach. Security professionals may think they can handle the effort, but they should turn it over to their PR people and executive management and work with them to ensure everyone understands all pertinent details. Doing this right can save an organization's reputation and even, in some cases, enhance the perception of its brand in the eyes of customers and the general public, said Ross Levanto.

In 2011, which Levanto called "the year of the breach," organizations learned that attacks are inevitable. The only good thing about the rampant activity, said Levanto, is that everyone now expects breaches to occur. Even so, companies should follow these straightforward but strict rules when addressing the media and the public:

- **Get it over with**
- **Be humble**
- **Don't lie**
- **Say only what needs to be said**

Breaches attract more attention than other technology-related topics, so reporters are more apt to cover them to drive traffic to their sites. If news organizations learn about these attacks through third-party sources while the breached organization remains silent, the fallout will be significant. Organizations must be proactive in their PR approach, using public messaging to counteract inaccuracies and tell the story from their point of view.

Following the Epsilon breach, according to Levanto, CEO Bryan Kennedy made the decision to go public with the story even though they weren't legally required to do so, as only email addresses, and not social security or payment card numbers, were stolen. He reasoned the news would get out anyway, so decided to proactively release details of the attack.

Don't wait until a breach happens to develop a PR preparedness plan — communications should be part of any disaster preparedness strategy. Security specialists should work with PR people to identify the worst possible breach scenario so they can message against it, and determine audience targets, including customers, partners, employees, and the media. Following a breach, messaging should be bulletproof and consistent, which requires that one person take the lead in PR interactions. As for who should take that lead, thinking has changed, said Levanto. Historically, the messenger has been a mid-level manager, but the nod increasingly goes to high-level executives like the CEO.

Today, there are numerous channels for PR outreach, and messaging should be consistent across all of them. Levanto said companies should set up Twitter feeds for their corporate brand and their offerings, and continually monitor feeds to see what customers are saying. Social media can serve as an early-warning system for breach activity. Further, security officers should set operational ground rules for employees that take effect in the case of a breach. For example, have them shut down Facebook, Twitter, or other means they could use to leak information before the organization's ready to go public.

## Covering your Assets

If the events of 2011 confirmed the belief that cyber-breaches are inevitable, your organization's leaders should have already examined existing insurance policies to see how they cover cyber-risk. Given the recent SEC ruling that public companies must disclose their cyber-liabilities and their risk protections, many are exploring cyber-insurance options.

While your organization's existing insurance policies will likely cover at least some cyber-related damage, said Scott Godes, it makes sense to consider overlapping cyber-insurance coverage. The seemingly innumerable variables that come with doing business in an online world demand that such policies be examined in the context of the industry vertical, affiliated partners, contractors, employees, IT infrastructure, data locations, customer locations, and other factors.

Cyber-insurance as it exists today "is a different animal than traditional insurance — nothing's regulated in these policies to date," said Godes. And because insurance providers view this coverage as a huge growth segment, they're rushing to develop new policy types.

Cyber-attacks complicate the already complex process of insuring a business. Take the issue of third-party vs. first-party risk. In its 2011 breach, Sony had to deal with both first-party and third-party damages. Sony makes a considerable sum through monthly fees and add-on sales for its Playstation 3 network, and during the weeks the network was down, the company lost an estimated $170 million in revenues, said Godes. This first-party damage has since been compounded by numerous third-party class action lawsuits filed by customers whose payment card data was exposed.

Considering the current unsettled state of cyber-insurance, Godes recommends a careful examination of existing policy coverage and that offered in new cyber-insurance contracts. Risk managers, privacy managers, legal personnel, and CIOs should all provide input. Insurance providers will demand that the organization prove it complied with specific security requirements before they will cover damages, so IT security team involvement is critical.

**Takeaway: Federal law enforcement dedicated to cybercrime is understaffed relative to the enormity of the threat, but agencies are making headway.**

Like the leaking of compromised data, financially motivated theft has come a long way, said Poulsen. In the 1980s, a criminal might go through dumpsters to get carbon copies of credit card transactions, perhaps getting a few credit card numbers. With transactions all done electronically over a network and stored in databases, perpetrators can now grab millions of numbers at a time.

Using such malware as Zeus, they can also snag online banking credentials and remote-control user machines to unprecedented financial advantage, said presenter Brian Krebs. Through cybercrime rings sourced primarily in Eastern Europe, organized syndicates recruit participants down to the level of money mules, who facilitate money-laundering activities by initiating wire transfers of money stolen through malware intrusions.

Fighting this rampant activity falls primarily on the shoulders of federal law enforcement agencies such as the USSS and FBI, who in turn must rely on state and local law enforcement, cyber-security forensics groups, and victims. In the case of the Secret Service Cyber Intelligence Section (CIS), conducting cybercrime investigations requires a great deal of diplomacy and arduous work. With 22 foreign offices, the unit has agents embedded in locations worldwide with officials from such groups as SOCA, Europol, NHTCU, and the Latvian State Police.

"We're uniquely qualified to work these cases," because the need to be extremely nimble encourages the development of close intra- and inter-agency relationships, said agent Matt O'Neill. "We can call on each other in any situation."

The operations of cybercrime rings today, O'Neill said, are extremely professional and sophisticated, equally capable of stealing machine-resident data and data in-transit, including encrypted data. They tend to operate in a Russian-speaking infrastructure that ensures English-speaking cybercriminals — and law enforcement — have little access capability. Through their own security measures, they understand vulnerabilities in wireless networks and point-of-sale machines, exploitable both through technology flaws and human complicity.

"There's a ton of money involved in these breaches and the groups involved spend it as quickly as they make it," said O'Neill. Why should anyone who hasn't been breached care? Because not only do these crimes harm businesses by decreasing confidence in online transactions, they threaten the U.S. financial infrastructure. Moreover, the money stolen is used to fund narcotics trafficking, extortion, terrorism activities, and other organized crime.

Among those hardest-hit in the last few years is the retail sector, through POS terminal hacks, though the massive TJX breach — which O'Neill said resulted in the theft of 40 million card numbers and potential losses exceeding $50 billion — heightened security awareness and measures. In the POS cybercrime realm, hospitality and food and beverage establishments are the fastest-rising targets, with the latter group the victims of 75% of such breaches in 2010.

These latest POS attacks typically target client-based applications installed by a vendor or the owner, where nobody changed the default username and password, said O'Neill. Absent even this basic

security measure, and compounded by weak or nonexistent firewall rules, hackers can easily infiltrate a system and install a keystroke logger. Almost half of such breaches involve malware exfiltration.

"Last year was a historic year in data breaches, completely changing the landscape," said Ostertag, who works with the USSS on the annual Verizon Data Breach Investigations Report. The groups tracked 761 cases in 2010, a considerable increase from the 141 cases in 2009. However, considering the big increase in cases, the number of individual records stolen in breaches was surprising: only 3.8 million individual records vs. 143 million in 2009, and 380 million in 2008.

Ostertag believes the increased number of breaches vs. the lower number of records stolen can be attributed to a couple of factors. One theory is that the market is glutted with payment card numbers thanks to frenetic Zeus activity over the last few years. Another is that criminals that focus on payment cards are keeping a lower profile due to arrests, moving from large data breaches to target more "mom and pop" shops with older POS systems, where they use point-and-click tools to get default passwords and steal card numbers. They may only get a few hundred records in an attack as opposed to thousands or millions, but they're hitting a much larger number of targets.

Further, when Verizon analysts checked mid-year 2011 breach data, they saw increased theft of corporate data rather than the usual large increase in payment card cases. Targets included intellectual property, particularly information on the processes that companies use to differentiate themselves from competitors. Following the Deepwater Horizon oil spill, for instance, numerous oil companies updated their own disaster plans — and many had them stolen.

The USSS has gotten increasingly adept at capturing these criminals, said Ostertag, and when perpetrators see their competitors arrested, they're motivated to choose other targets. "They figure there's less chance of arrest if they're stealing the intellectual property of one company rather than stealing millions of credit card numbers," he said.

Law enforcement has had some significant successes over the last couple of years, said Krebs. For example, in late 2010 the UK arrested 19 people central to an organized ring that used the Zeus banking trojan to steal $30 million from UK banks. At the same time, authorities in NY announced they were filing charges against 37 J-1 money mules, who ostensibly come to the U.S. on work-study visas but use their time aiding illegal money-laundering activities originating in their home nations.

"The NY operation was a big win for the Department of Justice because the criminals were all J-1 mules," said Krebs. "They can transfer a lot more money than regular money mules because they open bank accounts and tie them to fictitious companies, which fraudsters then use to launder money and recruit new money mules." Similar operations, he added, are underway in every major city in the U.S.

## Takeaway: Community outreach programs raise awareness of the impact of cyber-bullying by educating school administrators, parents, children, and the larger community.

Though financial and reputational damage from cybercrime occurs at the business level, awareness of the impact of harmful cyber-activity needs to start much earlier. Given the rampant cyber-bullying activity occurring among youth around the world, education should begin with school administrators, parents, and children, said presenter Phil Fogelman.

Technology, through the anonymity it enables, provides the same fertile breeding ground for cyber-bullying as it does cybercrime. And like cybercriminals, cyber-bullies don't empathize with their victims because the invisibility provided by the Internet allows them to disengage. This activity takes place everywhere on the Internet, both in peer-to-peer interactions and in social media, where anyone can "watch." Social networks, gaming sites, and discussion boards are all used to broadcast hurtful, defamatory, and even threatening comments, while texting and instant messaging deliver more-private attacks. The effects, said Fogelman, are far-reaching and socially devastating.

> **"Educate youth and encourage them to be allies with their peers against cyber-bullying activity."**
>
> **– Phil Fogelman, World of Difference Institute**

If the severity of a cyber-attack is high, law enforcement may bring charges based on digital evidence, but today, laws addressing cyber-bullying are still in the embryonic stage. Legislators and judges, much as they have with cybercrime cases, are struggling to make sense of the intricacies associated with bullying based in cyberspace.

Fogelman said it's imperative that school systems and parents work together to develop policies and education programs to protect victims against these activities, both to create a safe learning environment and to avoid civil action. Education should be extended to the larger community, so that everyone understands they have a responsibility to promote online safety, monitor online activity and depending on severity, report cyber-bullying incidents. Programs that promote peer-to-peer education are particularly effective.

"Educate youth and encourage them to be allies with their peers against this type of activity," Fogelman said.

## Takeaway: Get serious about a strategic security awareness program that makes every member of your organization a core member of the security team.

Because employees often create an environment ripe for hacks, they must understand their critical role in their organization's security effort.

"Security is everybody's business, so we need to get serious about security awareness," said Gamblin. He recommends developing awareness programs that train existing employees, incoming hires, and affiliated personnel on baseline security measures and making it clear that they're considered core members of the security team. For his part, Gamblin launched an effort in 2011 that targeted every member of the Missouri House of Representatives who was using gmail and put them through a two-factor authentication implementation process using Google Authenticator.

"Security awareness is a huge differentiator that security people neglect because it's not hardware, it's not shiny, and it's not sexy," said Gamblin. "But they have to develop awareness, as it's critical to security. You can do a lot to secure your company just by bringing groups together and helping them strengthen their Facebook and gmail account credentials and internal network passwords."

Other personnel processes to implement as part of security awareness program:

- **Formally identify any "splinter" group sites tangentially connected to your business.** By identifying associated sites, like a union site, you can help them address vulnerabilities that directly impact them and indirectly, your organization. "If an affiliated group's site gets hacked, news organizations and the public won't differentiate that the compromised server was outside your group — you'll get nailed, too. So it benefits you to help these groups as much as you can," says Gamblin.

- **Read content posted by prominent security journalists**. Follow the coverage of writers like symposium presenters Kevin Poulsen and Brian Krebs and other high-profile industry journalists.

- **Follow the Twitter feeds of Cisco, Microsoft, and other "bigs."** If you're using products from these providers, they have Twitter feeds specific to product lines where they announce vulnerabilities, usually in advance of other channels.

- **Phish your employees.** Testing your employees by offering up something tempting to see how willing they are to violate security policies is a great way to find weak spots and use your findings for educational purposes.

- **Penetration testing**. If you don't do penetration testing, hire a penetration-testing services provider to audit your security measures and test your network annually if not more frequently. If you do perform your own penetration tests, have a services provider double-check your findings. Do this not just to vet your own tests, but to ensure that you, as the security leader, don't make the common mistake of not documenting an issue because you know the idiosyncrasies of your IT environment.

# Advisories & Guidance

To stay informed on the latest cybercrime threats, as well as activities on the part of law enforcement, financial services, and other organizations, visit:

- **The Financial Services – Information Sharing and Analysis Center (FS-ISAC)**, which includes the Online Fraud Working Group: *http://www.fsisac.com*
- **Local FBI offices**: *http://www.fbi.gov/contact-us/field/field-offices*
- **The Internet Crime Complaint Center (IC3), a partnership between the FBI, National White Collar Crime Center (NW3C), and Bureau of Justice Assistance (BJA)**: *http://www.ic3.gov/default.aspx*
- **National Cyber-Forensics & Training Alliance**: *http://www.ncfta.net*
- **US-CERT (United States Computer Emergency Readiness Team)**: *http://www.us-cert.gov*
- **InfraGard**: *http://www.infragard.net*
- **Anti-Phishing Working Group (APWG)**: *http://www.antiphishing.org*
- **Maine Anti-Phishing Coalition (MEAPC)**: *http://nophishing.org*
- **World of Difference Institute**: *http://www.adl.org*

***For more information on the CyberCrime 2011 Symposium, visit cybercrime2011.com or sagedatasecurity.com.***

www.cybercrime2011.com