peer to peer MAGAZINE

SECURITY IS EVERYONE'S BUSINESS

Read this issue on the go!
A digital version is available for your tablet, smartphone and computer. Find more information online at **iltanet.org/p2p**.

***Peer to Peer* Magazine** is the quarterly publication of the International Legal Technology Association. Find out more at **iltanet.org**.

FALL 2014
Issue 3 Volume 30

What's the one tip you'd offer on how to improve security in an organization?

INCORPORATE TECHNOLOGY, STRATEGY AND ALLIANCES

name . . . . . Terry Aurit
company . . . . . Savvy Training & Consulting
website . . . . . www.savvytraining.com

Think **TSA**! It's not always the most pleasant experience, but the TSA has managed to keep millions of people and assets safe from external threats. You need a similar program, without involving any latex gloves or full-body scans.

- **T – Technology:** Obviously, utilizing technology to evade threats is vital. Are you deflecting malware before it has a chance to infect the organization?
- **S – Strategies:** Will you be able to anticipate and possibly recover from breaches? Do you have a plan in place?
- **A – Alliance:** People are your weakest link! You must form an alliance with each and every person who has access to your premises or your work product. Do you have policies regarding locking down firm laptops? Can the cleaning crew access the contacts in a desktop Rolodex? Are you viewing a sensitive document while in an airport or other public area?

The technology and strategic plans are vital, but you must continually communicate with the people in your organization to remind them of risks. Imprint the image of an airport security line to remind them why it takes a strategic alliance, coupled with technology, to reduce the chance of a disaster. P2P

DEVELOP AN INCIDENT RESPONSE PLAN

name . . . . . Doug Brush
company . . . . . Kraft & Kennedy, Inc.
website . . . . . www.kraftkennedy.com

It's not a matter of *if*, it's a matter of *when* you will experience an incident that impacts the confidentiality, integrity or availability of your data. While preventive and detective controls are important in mitigating threats, it is just as important to have an organized response plan to accurately determine if an event is actually an incident so you can take the necessary steps to control the situation and get the impacted resources in production again. The more disorganized your response efforts are, the more time, money and resources are lost getting the situation under control while also increasing the risk that the issue is spread to other systems. Make sure your incident response plan has the right resources such as call trees, secure communication channels and trained staff in place well before an incident so the mean time to respond (MTTR) can be reduced to levels that allow your team to respond fluidly to the situation. Also, it's important that your team document all actions during a response so the process can be reported to management and serve as an educational tool to improve future response efforts. And remember: Stay calm! P2P

MAKE USERS AWARE

name . . . . . Joseph Marquette
company . . . . . Accellis Technology Group
website . . . . . www.accellis.com

The number one tip is awareness. Firm members have to know what risks exist, what actions to avoid and what to do if they think something is wrong. All the technology in the world can't help you if a secretary connects a virus-laden thumb drive to her desktop!" P2P

***Want to appear in the next* Peer to Peer?**

Here's the question for the Winter edition on all things mobile, virtual and cloud-based:

What one technology is revolutionizing connectivity? (think lawyers connecting to clients, users connecting to info, staff connecting across global offices, etc.)

Send your answer to ***kristy@iltanet.org***

THE DATA BREACHES ARE COMING

It is not a matter of whether you will experience a data breach; it is a matter of when you will experience one. An incident response program can enable your cybersecurity program to recover quickly from incidents and mitigate the potential for reputational and financial harm.

TYPES OF ATTACKERS

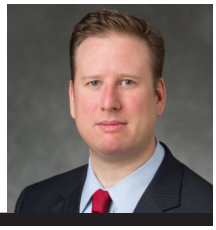
In the past, when people thought about their computers and networks being attacked, they often pictured characters from TV shows with dark sunglasses, wearing all black and boasting to their friends about their exploits. But in the modern threat landscape, attackers are typically motivated by financial or political concerns rather than by bragging rights. Attacks can come from inside or outside your walls, and you need to know the types of threats you will likely face.

- **Insider Threats:** The human capital in a law firm is its biggest asset but is also its greatest risk. Once inside and authorized on a network, employees have a wide range of access to information and resources. Insiders can take data, use technical resources against company policy or even use the firm's email system to harass people. In addition, third parties such as contractors or vendors with access to firm resources and insight into firm operations can often be a blind spot in the threat landscape because they may not be monitored as closely as internal personnel.

- **External Threats:** Many kinds of external attackers pose threats to computers and networks, from the simplest automated scanning bot-nets to so-called script kiddies (unskilled individuals exploiting known vulnerabilities with little understanding of what they

About the Author

Douglas Brush is the Director of the Information Security and Governance practice in the New York office of Kraft Kennedy. Douglas is an expert in digital forensics and cyber-investigations. He leads investigations into hacking, data breaches, trade secret theft, employee malfeasance and financial fraud. In addition to advising on compliance, Douglas assists clients with information technology security assessments, digital forensic investigations, and incident response programs. Contact him at brush@kraftkennedy.com.



are doing) to hacktivists to hacking groups and nation-state Advanced Persistent Threat (APT) actors. As we move into a more connected world, with more resources connected to the Internet, the surface area for external attacks grows and grows. It is important to be able to understand an external attack so you know where it is coming from. You also need to know the potential skill level of the attacker so you can better respond to events and reduce the harm to your environment.

HOW AN ATTACK HAPPENS

Each type of an attacker uses different methods to compromise an IT asset to perform actions or steal data. Be familiar with the different steps an attacker will take so you know where to better identify vulnerabilities and be proactive about remediating weaknesses before they are exploited.

- **Reconnaissance:** Reconnaissance is the actions an attacker takes to "case the joint." This information gathering can be done by reviewing your own website, social media platforms, databases such as Public Access to Court Electronic Records (PACER), database lookups using Whois.net, and domain name system (DNS) records, and advanced tools to mine and correlate data.

- **Scanning:** Scanning techniques use networks and networking technology to identify connected IT assets. The most common form of scanning uses tools to probe TCP/IP networks to map computers, routers and servers, identify the devices' operating systems and discover open ports and services. Because this method relies on the way networks and the Internet work at the most basic level, it is also used by system administrators for monitoring. In fact, network scanning is built into many free and commercial network vulnerability assessment tools. Another scanning technique involves wardriving, which scans for wireless networks and captures information about the wireless signal strength, channel and security. This again can be used for good or evil purposes, depending on who is doing the scanning.

- **Exploitation:** Exploitation is an active attempt by an attacker to get a toehold in a system or network. This can come in the form of phishing email, a USB flash drive or a compromised host with a known vulnerability. The attacker may even try multiple methods on multiple systems or people in an organization to increase the likelihood of successful exploitation.

- **Maintaining a Presence:** Attackers who get in want to stay in and be unnoticed. After a successful initial exploitation, an attacker scans an environment for new targets, harvests credentials, escalates privileges and pivots to new systems to exploit. The attackers try to blend in with regular user activity to maintain a low profile. They may also go to great lengths to obscure their actions by deleting files and logs. They may also hide in plain sight by placing malware in common operating system directories with file names that look like operating system files.

- **Exfiltration:** In most common breaches, attackers are attempting to remove data from its environment. This is called exfiltration. Exfiltration can be done by insider threats with USB flash drives, cloud storage platforms such as webmail or cloud storage or even something as simple as printing confidential documents and walking out the door. External threats continue to use methods such as outbound email services, file transfer protocol (FTP), key stroke logging and channeling of traffic through common Web service Internet ports 80 and 443 (SSL). The use of port 443 is especially difficult to detect because the traffic is encrypted.

4 Tips for Successful Incident Response

1. *Have a plan. Make sure your organization has a documented set of policies and procedures.*
2. *Stay calm. Adding further anxiety to a stressful situation impedes response efforts.*
3. *Document. Include everything done in the response effort. It's easy to forget key details for a report.*
4. *Use outside advisors. Seek outside counsel to maintain privilege. Contact your business insurance broker to see which costs can be absorbed by your policies.*

AN INCIDENT RESPONSE PROGRAM

With an understanding of the types of attackers and their methodologies, we can be better prepared to respond. The key is to be prepared to respond, not to react. Many incidents could be active for days, weeks or even months. Without a properly formulated plan, you risk ruining your chance to properly understand what has occurred, identify how many systems are affected and determine who is responsible. To address an incident, you need to know how to properly escalate an event, call on the right people and have a structured incident response (IR) program.

- **Planning and Preparation:** The first step in setting up an IR program is to create the response plan: a documented set of policies and procedures that the organization follows when addressing an incident. The plan should detail who is involved at what stages and give detailed contact information. Such information can include C-level, general counsel, outside counsel, business unit leaders, system and network administrators, outside forensic vendors and even your cybersecurity insurance broker. The plan should also include a meeting place that has adequate power, privacy, communication lines and white boards. Part of your preparation should include go bags or jump kits that are ready at all times with forensic disk imagers and boot discs, disk drives for data storage (you don't want to scramble to source a two terabyte hard drive at three a.m.), network taps, printed procedures and call trees. Make sure people are properly trained for IR procedures, and conduct regular response drills.
- **Detection and Analysis:** If you monitor your network and hosts regularly, you will see more and more alerts and events. However, not every event is an incident, and it is important to know your normal environmental baselines. Know where to look on your network perimeter, host perimeters, file systems and applications to aggregate data points and be able to make the proper determination that there is an incident. Once you can make the call that there is an incident, ensure there is someone to quarterback the process and act as the lead incident handler. Also, be discreet. More advanced attackers will be monitoring and will react to your awareness of their activity. Consider using out-of-band communications, and act on a need-to-know basis.

- **Containment, Eradication and Recovery:** Once you have determined there is an incident, you need to characterize the incident type and assess its severity and sensitivity. You will need to inform management, practice leaders and possibly law enforcement. Employ forensic best practices for gathering evidence, and capture information from RAM, hard disks and monitoring systems. You may have to isolate the system from the network or even power the system down to prevent further compromise. Also, consider applying patches, changing passwords and modifying firewall rules. Once you have the situation controlled, you can move into deeper analysis of the data while you remove an attacker's artifacts or even wipe and reload the systems. Work with the business owners to ensure that the previously compromised systems are performing as expected once they are back online. The systems should then be monitored to watch for attackers trying to compromise them again.

- **Post Incident:** After the incident has been adequately dealt with, it is time to review what happened and make necessary changes to your environment. A report of the incident should communicate the nature of the event and what actions were taken to respond to it. The report should have an executive summary with supporting appendices so it is easy to digest, and it should be presented soon after the remediation of the incident. If the report identifies organizational vulnerabilities where risks can be proactively mitigated, this may be an appropriate time to ask for additional security program funding. Any weaknesses in your incident response program that the report identifies should be used to improve the process.

Information and knowledge are the lifeblood of law firms. Firms continue to gather client data and rely on technology to respond to client demands in an always-on, always-connected world. An attendant risk of data breaches occurs because firms have more information in more places with more inbound and outbound traffic on their networks. Taking proactive defensive measures to structure your environment to prevent attacks and monitor vulnerabilities is critical for reducing the risk attackers pose. Just as important is knowing how to detect and respond to attacks when they occur. Remember it's not a matter of if; it's a matter of when you will be breached. P2P