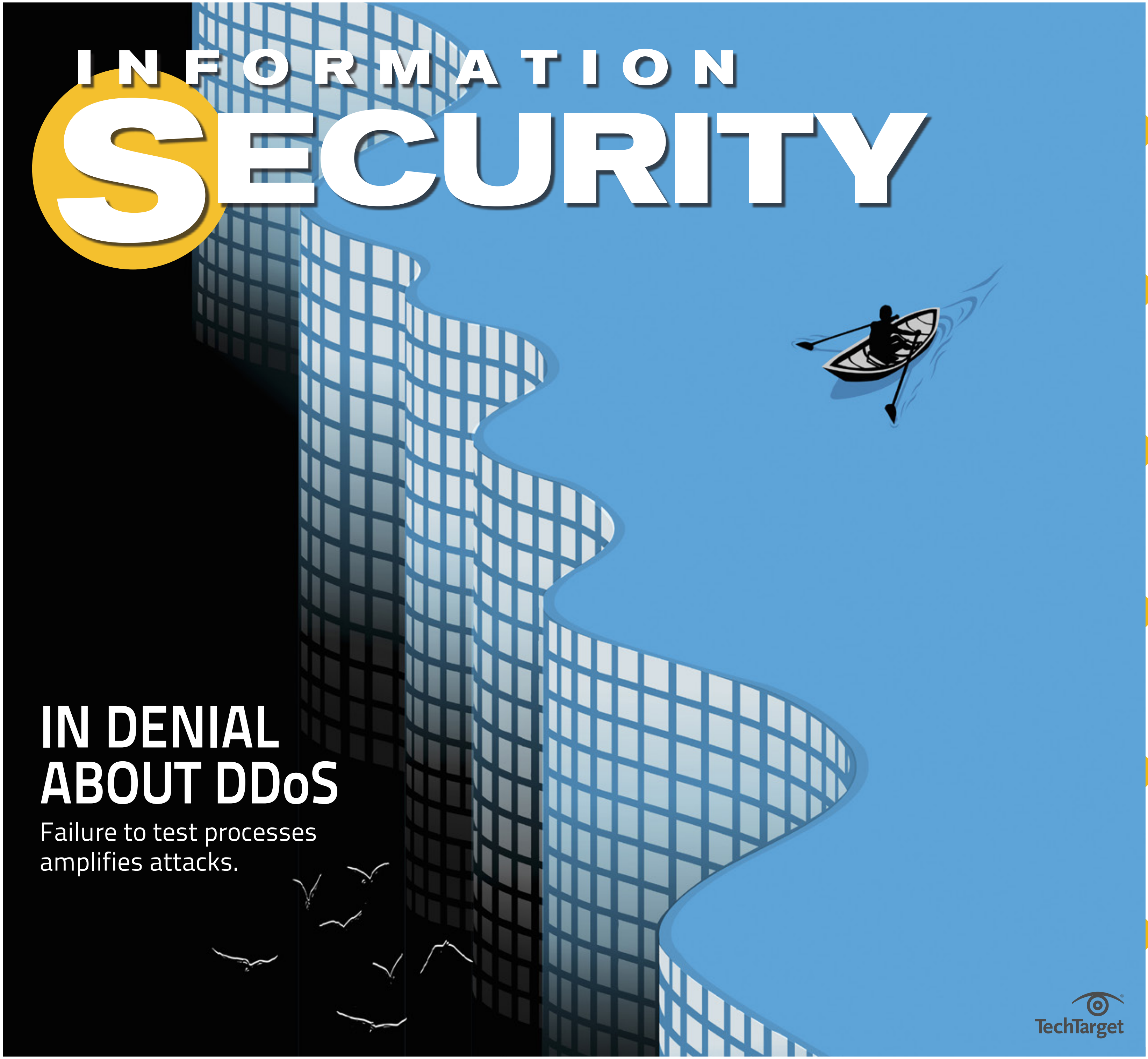
INFORMATION SECURITY

FEBRUARY 2015
VOL. 17 | NO. 1



IN DENIAL ABOUT DDoS

Failure to test processes amplifies attacks.

TechTarget

The Politics of DDoS Response

Reports of a 'hack back' DDoS attack by Sony stirred up acceptable use questions.

BY KATHLEEN RICHARDS

D**ISTRIBUTED DENIAL-OF-SERVICE** attacks are generally designed to prevent legitimate users from accessing a website or service. Advanced DDoS attackers are increasingly using a customized mix of techniques to attack targeted victims in ways all too similar to advanced persistent threats, says John Pescatore, director of emerging trends at the SANS Institute. He looks at the current denial-of-service landscape and associated costs in his article "DDoS Defense Planning Falls Short."

But what would happen if the tables were turned?

In early December, reports of a "hack back" DDoS attack by Sony stirred up acceptable use questions. Two unnamed sources told Re/Code that Sony was using hundreds of computers in Asia to launch DDoS attacks against sites that had posted stolen data from a breach at Sony Pictures Entertainment in an attempt to block access to intellectual property (movies) and other sensitive data. Security analysts without direct knowledge of the DDoS attacks pointed to torrent poisoning, which soon followed, as the more likely scenario. DDoS is illegal and against most Internet service providers' acceptable use policies, which would prohibit companies like Sony from using these tactics, they argued. But are people who are accessing stolen property and data legitimate users of websites?

How far should companies be allowed to go to protect their intellectual property and employee data against further exposure?

HOME

EDITOR'S DESK

DDoS DEFENSES

BIG DATA ANALYTICS

CISO TECH ASSESSMENTS

DATA SECURITY

A CHAT WITH DIANA KELLEY

SECURITY EDUCATION

Sony's ongoing security woes—the PlayStation Network was DDoSed on Dec. 25 and was slow to come back online—have unleashed a hornet's nest of security concerns and hotly debated issues: How far *should* companies be allowed to go to protect their intellectual property and employee data against further exposure after a hacking incident and extortion that resulted in a seismic data breach?

These questions are focusing more attention on data-driven security projects in 2015. In the February issue of *Information Security* magazine, authors Adam Rice and James Ringold outline the promise of using data security analytics to track the APT lifecycle in their article, "Man Versus Machine Data." The hard issues around intellectual property protection and the steps enterprises and vendors are taking to address them are covered in my article,"Heat from the Breach."

The heightened attention going forward on information security will bring new opportunities for security professionals. But as most IT security managers know all too well, once intellectual property and PII is in the wild, all bets are off. ■

KATHLEEN RICHARDS *is the* Information Security *magazine features editor. Follow her on Twitter* *@RichardsKath*.

DDoS DEFENSE PLANNING FALLS SHORT

Failure to regularly test DDoS mitigation processes can lead to inadvertent amplification of an attack.

By John Pescatore

GAMERS LAST CHRISTMAS got an unwelcome surprise when distributed denial-of-service attacks prohibited them from using the Microsoft Xbox Live and Sony PlayStation networks. While customers were disappointed, the bigger shock may have been how long the outages lasted. Denial-of-service attacks have caused serious disruptions for over 15 years, but a 2014 SANS report showed that 40% of enterprises remain unprepared to mitigate such attacks and recover business services. Almost one in four didn't even have a plan in place at all. Since the same report showed an average of over four DDoS attacks per year, unprepared companies are at high risk of business interruption—as Sony learned when its PlayStation Network was brought down and remained offline for several days.

Having a response plan is a start, but of those enterprises that did have DDoS mitigation processes in place, fewer than 50% had tested those capabilities. Failure to regularly test those processes can lead to inadvertent amplification of an attack. When one large enterprise came under fire and switched its network traffic to a contracted cloud-based DDoS mitigation service provider,

HOME

EDITOR'S DESK

DDoS DEFENSES

BIG DATA ANALYTICS

CISO TECH ASSESSMENTS

DATA SECURITY

A CHAT WITH DIANA KELLEY

SECURITY EDUCATION

the company lost all connectivity to the Internet—a problem that would have been found and solved earlier with minimal interruption if the enterprise security team had tested the switchover process.

And denial-of-service interruptions aren't just problems for financial institutions and gaming networks. DDoS attacks are spread across all industries and company sizes and happen at all times of the year. A 2014 report by data security provider Incapsula, now a division of Imperva, showed a 240% increase in bot-based DDoS attacks over 2013. Reports by other service providers show similar statistics, with the intensity and complexity of DDoS attacks growing along with the sheer number of attacks. The motivation for the attacks ranges from hactivism to extortion, with attackers often threatening to escalate the attacks if payments are not made.

The bottom line is that denial-of-service attacks represent a high risk for almost all enterprises. Proper planning for DDoS mitigation requires cooperation between IT, network operations and security groups. CISOs need to play a leadership role in making sure DDoS mitigation and response processes and responsibilities are defined, understood and regularly tested.

> The motivation for DDoS attacks ranges from hactivism to extortion, with attackers often threatening to escalate the attacks if payments are not made.

NOT JUST BRUTE FORCE ANYMORE

Cyberthreats evolve at pretty much the same pace as technology, and denial-of-service attacks are no different. The Morris worm of 1988 used simple exploitation of well-known operating system vulnerabilities in VMS and SunOS to take down close to 25% of the servers connected to the Internet. In February 2000, Amazon, eBay, Yahoo and other sites were hit with brute force DoS attacks. The Code Red/Nimda and Slammer/Blaster worms of 2001 and 2003 used slightly more sophisticated techniques to exploit unpatched Windows PCs and servers and cause widespread denial of service of millions of PCs and servers.

The earliest denial-of-service attacks were not complex, and mitigating them was relatively simple. Since the attacks came from a small number of sources, basic IP address blocking could be used, ideally at the Internet service provider (ISP) level, but even at the perimeter firewall or load balancer. However, by 2005, attackers began to launch DDoS attacks, using hundreds and thousands of compromised PCs and servers (botnets) to act as denial-of-service relays. DDoS attackers eventually added fast flux DNS techniques, which enabled botnets to rapidly and continually change source IP addresses.

DDoS mitigation vendors and service providers began to add detection techniques to augment IP address blocking by using rate-based anomaly capabilities and signature detection of common flood techniques to differentiate high volume traffic from DDoS attacks. This caused attackers to up the ante in both sheer bandwidth and frequency of occurrence. They also began to research the application logic of the target's websites.

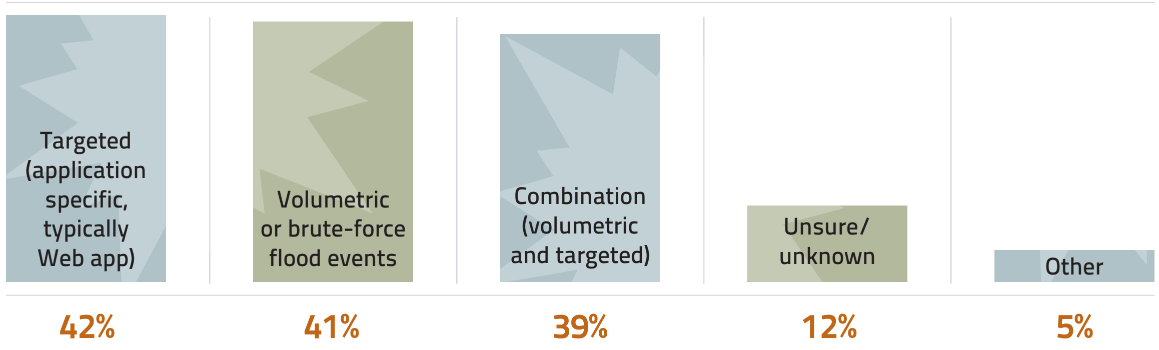
A new form of DDoS attack known as "resource depletion" attacks consumed all of a server's processor cycles or memory space without requiring high volumes of traffic from the attacker. These types of attacks start user authentication processes, launch site-wide searches or initiate multiple account creation processes to bring server response to a crawl or even crash the target server. The result is denial of service that evades rate-based detection techniques.

Advanced DDoS attacks blend all of these techniques. That is what can make the detection of them difficult and the response planning even more so. A brute force flood attack can usually be handled purely by the network operations group, while application-layer attacks generally require cooperation by application owners, database analysts and webmasters.

The "Operation Ababil" attacks against U.S. banks in March 2013 combined three attack techniques to get

Types of Attacks

What types of attacks did you experience? (Respondents could select all that apply.)



SOURCE: DDoS ATTACKS ADVANCING AND ENDURING: A SANS SURVEY, FEBRUARY 2014

HOME
EDITOR'S DESK
DDoS DEFENSES
BIG DATA ANALYTICS
CISO TECH ASSESSMENTS
DATA SECURITY
A CHAT WITH DIANA KELLEY
SECURITY EDUCATION

around DDoS defenses:

- DNS query application-layer attack
- GET and POST application-layer attacks on both HTTP and HTTPS
- Brute force using UDP, TCP Syn floods, ICMP and other IP protocols

The mix of techniques does not remain constant, which creates more challenges for DDoS reponse planning and testing. Cloud-based DDoS mitigation provider Prolexic's Quarterly Global DDoS Report showed that the use of application-level attacks decreased in Q2 2014 after high levels of growth in previous quarters. Over the same period, infrastructure or flood-based attacks increased again.

Attackers tailor the mix of these attack "primitives" to create threats that are customized for the intended target—much the same way advanced targeted attacks (often called advanced persistent threats) create customized malware to breach enterprise defenses.

DISRUPTIONS AND DAMAGES

While simple DDoS attacks may cause more annoyance than business interruption, the impact of today's more complex DDoS attacks is widespread. Initially, business services are interrupted for some period of time. There are other costs (response, cleanup, opportunity cost, brand reputation) associated with a DDoS attack, but for most businesses the interruption of revenue is the largest cost. The magnitude of that cost depends primarily on two factors: (1) the length of the outage and (2) the loss of revenue per unit time from unplanned downtime.

The unplanned disruption is experienced, often by customers, for the period of time that the DDoS attack goes unmitigated. The Prolexic report showed an average duration of 17 hours for DDoS attacks. The SANS survey indicated an average attack length of 8.7 hours.

Advanced DDoS attacks blend all of these techniques, which makes detection and response planning more difficult.

Organizations without DDoS defenses in place could experience down time for the entire duration of an attack: One enterprise, whose security management was interviewed for the SANS report, lost its Web presence for a full two days. However, organizations that can respond rapidly and mitigate a DDoS attack can reduce the length of the outage; the SANS report showed an average down time of 2.3 hours.

The cost of unplanned downtime varies widely by industry, company and business service. A 2013 Cost

HOME

EDITOR'S DESK

DDoS DEFENSES

BIG DATA ANALYTICS

CISO TECH ASSESSMENTS

DATA SECURITY

A CHAT WITH DIANA KELLEY

SECURITY EDUCATION

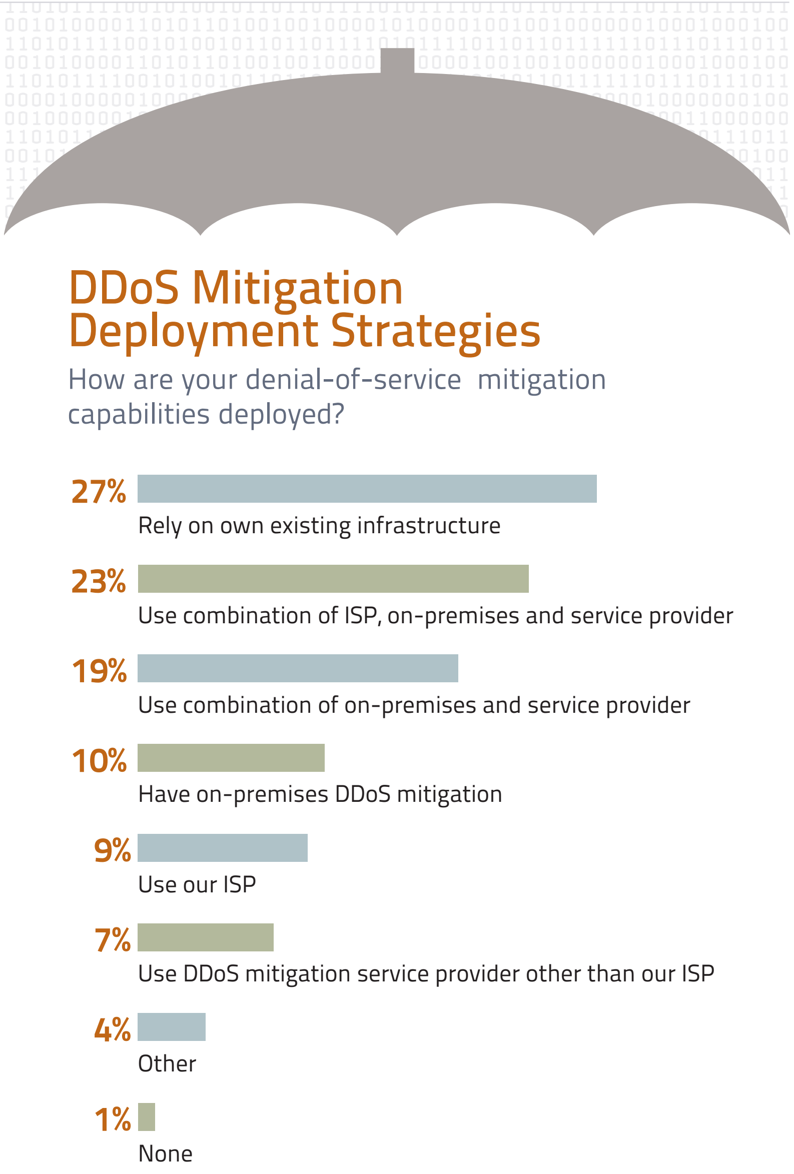
of Data Center Outages survey by the Ponemon Institute showed that the cost of a data center outage averaged $474,000 per hour. Gartner estimates a slightly lower cost of $336,000 per hour. For some businesses, a full data center outage may be more costly than a DDoS attack that only impacts Internet-exposed systems. However, many data center outages do not affect all Internet-facing systems, and for businesses in which revenue is tightly coupled to website availability, the cost of a DDoS outage may actually be higher than that of a data center outage.

For illustration purposes: If the cost of a successful DDoS attack is $400,000 per hour, then a 17-hour outage would result in an average business disruption cost of $2.8M. By mitigating that attack to the average 2.3-hour outage duration (shown in the SANS report), the business cost would be reduced to $920,000—a savings of almost $2M.

This analysis is analogous to the calculations CIOs must make around business continuity and disaster recovery investments. A successful DDoS attack is similar to a power outage or natural disaster that brings down IT systems; the event cannot be avoided but investments in processes and technology can be made to reduce the impact to an acceptable level.

MITIGATION STRATEGIES

Several approaches are available to enterprises for



DDoS Mitigation Deployment Strategies

How are your denial-of-service mitigation capabilities deployed?

SOURCE: DDoS ATTACKS ADVANCING AND ENDURING: A SANS SURVEY, FEBRUARY 2014

HOME
EDITOR'S DESK
DDoS DEFENSES
BIG DATA ANALYTICS
CISO TECH ASSESSMENTS
DATA SECURITY
A CHAT WITH DIANA KELLEY
SECURITY EDUCATION

reducing the effect of a DDoS attack. In order of increasing effectiveness, organizations should consider the following:

1. **Use of existing infrastructure.** Existing firewalls, routers, load balancers and other network components to mitigate DDoS attacks are rarely an effective solution, as even the lowest level DDoS attacks will likely overwhelm those resources and seriously impact network performance. However, for small enterprises that have over-provisioned these components, relying on the existing infrastructure to protect itself may be the only choice when budget constraints do not support any dedicated DDoS mitigation technologies.

2. **Local DDoS protection products.** DDoS mitigation appliances are sold by companies such as Arbor Networks, Corero Network Security, Fortinet and Radware. These products can be effective in keeping DDoS traffic from impacting your network and servers without affecting legitimate traffic, but since they operate at your end of the Internet connection, large-scale brute-force attacks can still consume all of your available Internet bandwidth and disrupt customer traffic.

3. **ISP "Clean Pipe" services.** All major ISPs (and Web hosting providers) offer DDoS mitigation services that provide service-level agreements for various levels of DDoS filtering. The performance of ISP-based DDoS mitigation services varies widely—the ISP your network group has selected may or may not be very good at DDoS filtering. If you have multiple ISPs in use, you will need to contract for services with each service provider.

4. **"Man in the Middle" DDoS mitigation services.** Companies such as Akamai Technologies, CloudFlare, Imperva/Incapsula, Neustar and VeriSign provide DDoS mitigation services from their cloud-based "scrubbing" centers. When you detect a DDoS attack, you reroute traffic through the DDoS service provider. The service provider uses a variety of techniques and technology to filter out the attack traffic and forward legitimate traffic to you. Another more expensive option is to have your traffic always flow through the service provider for fully automated detection and mitigation. This mitigation strategy is very effective but does

> Whichever approach to mitigation is used, CISOs must both define the processes followed once a DDoS attack is detected, and regularly test them.

HOME

EDITOR'S DESK

DDoS DEFENSES

BIG DATA ANALYTICS

CISO TECH ASSESSMENTS

DATA SECURITY

A CHAT WITH DIANA KELLEY

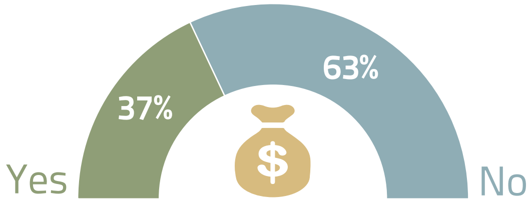
SECURITY EDUCATION

introduce additional latency and complexity into Internet connection and routing. This approach can be used to provide DDoS protection to cloud-based services, as well.

Which of these services is best depends on the architecture and configuration of your Internet connection. Large enterprises with complex use of the Internet, and trained staff, will usually find that a mix of some on-site DDoS mitigation capacity combined with the use of a cloud-based DDoS mitigation provider is the most effective and efficient approach. Smaller organizations may find that using ISP services is sufficient and requires the lowest expenditure in both procurement costs and staff training and time.

DDoS Defense Budgets

Do you carve out a percentage of IT budget for DDoS defense technologies/service providers?



SOURCE: DDoS ATTACKS ADVANCING AND ENDURING: A SANS SURVEY, FEBRUARY 2014

PROCESS, PROCESS, PROCESS

Whichever approach to DDoS mitigation you choose, CISOs will need to both define the processes to follow once a DDoS attack is detected and regularly test those processes—just as they have to do for disaster recovery services. Processes (and responsibilities) need to be defined in several areas:

- **Detection.** What parameters will be monitored to detect the onset of a DoS attack? What thresholds will be used on different business processes to determine if response is required?

- **Response.** The best response to an attack will vary depending on what systems are affected and what type of attack is underway. Response plans for critical systems should be defined as well as responsibilities for making decisions on engaging mitigation capabilities or disconnecting systems.

- **Reporting.** CISOs should define processes for notifying corporate management, business partners and customers, as well as for making the decision whether or not law enforcement should be involved.

HOME

EDITOR'S DESK

DDoS DEFENSES

BIG DATA ANALYTICS

CISO TECH ASSESSMENTS

DATA SECURITY

A CHAT WITH DIANA KELLEY

SECURITY EDUCATION

- **Lessons learned.** After an incident, processes should be reviewed and updated where required.

These processes will generally require a mix of security and network operations personnel, and often website administrators, as well as any third-party DDoS mitigation providers that are involved. Testing DDoS mitigation processes at least twice per year is necessary to ensure smooth operation when a real attack occurs. Ideally, DDoS processes should be tested at the same time as disaster recovery processes such as emergency power generators.

Nothing stays static in cybersecurity and DDoS attacks are no exception. Attacks will continue to increase in quantity, intensity and complexity. The next wave will likely include attacks against mobile devices and applications, and the use of vulnerable devices on the Internet of Things to launch even more widely distributed and complex attacks. Your ISP is a great source of information for the latest information on DDoS attacks, as are the periodic threat reports the DDoS mitigation providers put out. ■

JOHN PESCATORE *is director of emerging trends at SANs Institute. A former vice president and distinguished analyst at Gartner, Pescatore has over 30 years of experience in computer, network and information security. Prior to Gartner, he was senior consultant for Entrust Technologies and Trusted Information Systems and a security engineer for the U.S. Secret Service and the National Security Agency.*

MAN VERSUS MACHINE DATA

Without a trace: Cybersecurity incident response teams must follow the thread of security events through volumes of log data from increasingly diverse sources.

By Adam Rice and James Ringold

ORGANIZATIONS THAT START to address information security in a meaningful way will come to a point in their maturity when they have a lot of machine data. The challenge many CISOs face is how to leverage that data quickly and correlate events dynamically across the enterprise to track down advanced persistent threats (APTs). The Sony Pictures Entertainment hacking incident in November underscores the importance of security monitoring and rapid incident response to clamp down on damages before disaster strikes.

IT security managers cannot protect what they cannot see; and to "see" associations or patterns that can help detect APTs, enterprises must have comprehensive logging in place across multiple layers within a network. The greater the visibility, the larger the machine data, and the harder it is for cybersecurity incident response teams to "follow the thread" and correlate security events with threat intelligence in a meaningful way. The answers to many security questions about fraudulent activity, user behavior, communications, security risk and capacity consumption lie within these large data sets.

HOME

EDITOR'S DESK

DDoS DEFENSES

BIG DATA ANALYTICS

CISO TECH ASSESSMENTS

DATA SECURITY

A CHAT WITH DIANA KELLEY

SECURITY EDUCATION

Why so much logging? Most advanced adversaries gain access to a victim's network via malware, drive-by links or Web shells. Once the initial attack phones home—malware will initiate outbound connection to C2 hosts to get around inbound firewall rules—root kits are delivered, and they quickly gain access to a user account and drive around the network as a fully credentialed user. It is difficult to lock down a Microsoft network in any meaningful way without destroying its functionality. A successful strategy to defeat this type of attack includes the following:

- Detect the malware or drive-by links before users click on them. To do this a cybersecurity incident response team has to be able to compare user behavior against threat intelligence. This requires full packet logging of all ingress and egress traffic on an enterprise's edge.

- Detect malware or rootkit delivery to the endpoint. To do this the cybersecurity team needs verbose logging on antimalware and endpoint protection systems.

- The cybersecurity team needs to be able to analyze user behaviors and access across the entire enterprise. Security information and event management (SIEM) tools can alert you to unusual activity, such as account usage during off hours. This is only possible with comprehensive logging of Active Directory (AD) and host access events.

COMPREHENSIVE LOGGING

All of this logging can result in close to a million pings a day about potential security events at larger enterprises and terabytes of logging data a month. While comprehensive logging is needed, several factors have to be considered when you increase logging across the enterprise. Infrastructure that is already heavily utilized might experience performance issues with additional logging. The network team should be involved in the design of the logging infrastructure to make sure the aggregation of enterprise-wide logging does not affect performance when all log sources are pointed at a few destinations. It's important to involve key stakeholders in the design and to balance the need for logging with the function of the applications. To see across an enterprise, verbose logging should be enabled throughout as follows:

- Layer 2 switching and choke points on enterprise distribution switches.
- NetFlow enabled and logged where possible.
- Critical services to send access and systems' logs.
- AD to log user behaviors.
- All Internet-exposed devices to log access and system events.
- Endpoint protection systems to log alerts.
- All firewall devices to log inbound access (accepts) and outbound (accepts and denied).
- Other security devices to log alerts and access.

Most security programs begin with logs from the devices at the edge of the network, because those are usually easier to obtain. Firewall, network intrusion detection system and other network-based security products have robust and mature logging capabilities that most companies are already using. The level at which the logging is configured is paramount for visibility into the various APT traffic as it is leaving or entering your environment. This means that if there is an active intrusion, traffic coming and going from the network edge has to be correlated with the suspicious traffic to see the entire communications channel—malicious actors infiltrating the network, driving a compromised account, and then moving laterally across the enterprise. It's critical to be able to see both successful and denied traffic at the network edge to get a profile of what is normal for your business.

NETWORK CONNECTIVITY AND COMMUNICATIONS

At the network edge, be sure that your logging doesn't have additional blind spots to traffic that can be used to bypass your security controls. Encrypted traffic, such as SSL/HTTPS, and services that are traditionally used for communication and data transfer, such as IRC and FTP/SFTP/SSH, should also be logged with detail.

Logging of services available to the public Internet is also of great interest, as these systems are the gateways to and from your infrastructure. Any Web server should log not only the connections into the server, but also the actions and input within the applications, so you can understand if they are being used as a bridge to your network. This logging should include not only internally developed Web apps and services but also vendor-provided appliances and apps that reside on those systems. The logging needs to enable you to see what is behind all network communications to and from your environment.

Any security device or system software within your network should also create logs. These security systems usually include, but are not limited to, antivirus or other host intrusion detection software. You can review the host logs on the systems to gain an understanding of the network accounts and computer systems that are used within the scope of the threat. Host firewall logs can be critical to understanding how the threats are moving around within the network after an initial compromise.

Similarly to the host-based firewall logs, NetFlow can help monitor the traffic within your network and identify areas that require further investigation. NetFlow can alert your team to data-transfer activity that is happening within your network that might not be authorized or sensitive information that is being prepared for transmission outside of your network.

CENTRALIZED SYSTEM

Network authentication logs from AD and other LDAP-based services used for central authentication of users and network systems enable you to trace access within your environment and begin to frame up which systems are involved with the threat. Many of the applications and systems in this list will have the capability to send logs off to a centralized system, either through syslog or another facility. Having a central log collection and analysis system is crucial because trying to look in all of these systems, with multiple sources and locations, for the log information is tedious work. This log information will be written to system logs on the hosts, which systems administrators will want to constrain so the data doesn't consume usable system disk space. Security logs kept on systems will usually contain data for a few days at most, and in many situations only a few hours. This is not sufficient time to allow for analysis and review.

Most intrusions are not detected for months after the initial compromise (which may have been the case with Sony). An advanced attack usually goes unnoticed for more than a year, according to a 2012 report by Mandiant, now a division of FireEye, which is consulting on the Sony breach. If log data is not collected and retained during those months, the ability to identify the system of source or persistence is impossible, and the threat may remain within your network for a very long time.

BIG DATA PROBLEM

When the cybersecurity incident response team investigates an incident they must be able to follow the thread of events through logged data, and that path is interwoven through the Microsoft domain, security devices, edge devices, switches and routers. During a security event, time is essential in stopping the unauthorized exfiltration of data from a network. From the point of discovery to when an active defense is put in place and the adversary is stopped is a critical time.

To be successful in seeing, stopping and investigating a cyberevent, an enterprise must have the ability to quickly query very large sets of machine data. The notion of having a commercial off-the-shelf tool that has all the answers programmed into its graphical user interface is a fallacy. There is no fixed solution. Queries against large sets of machine data must be dynamic, and results must be presented quickly. For security analysts to be successful, they have to be able to manage big data.

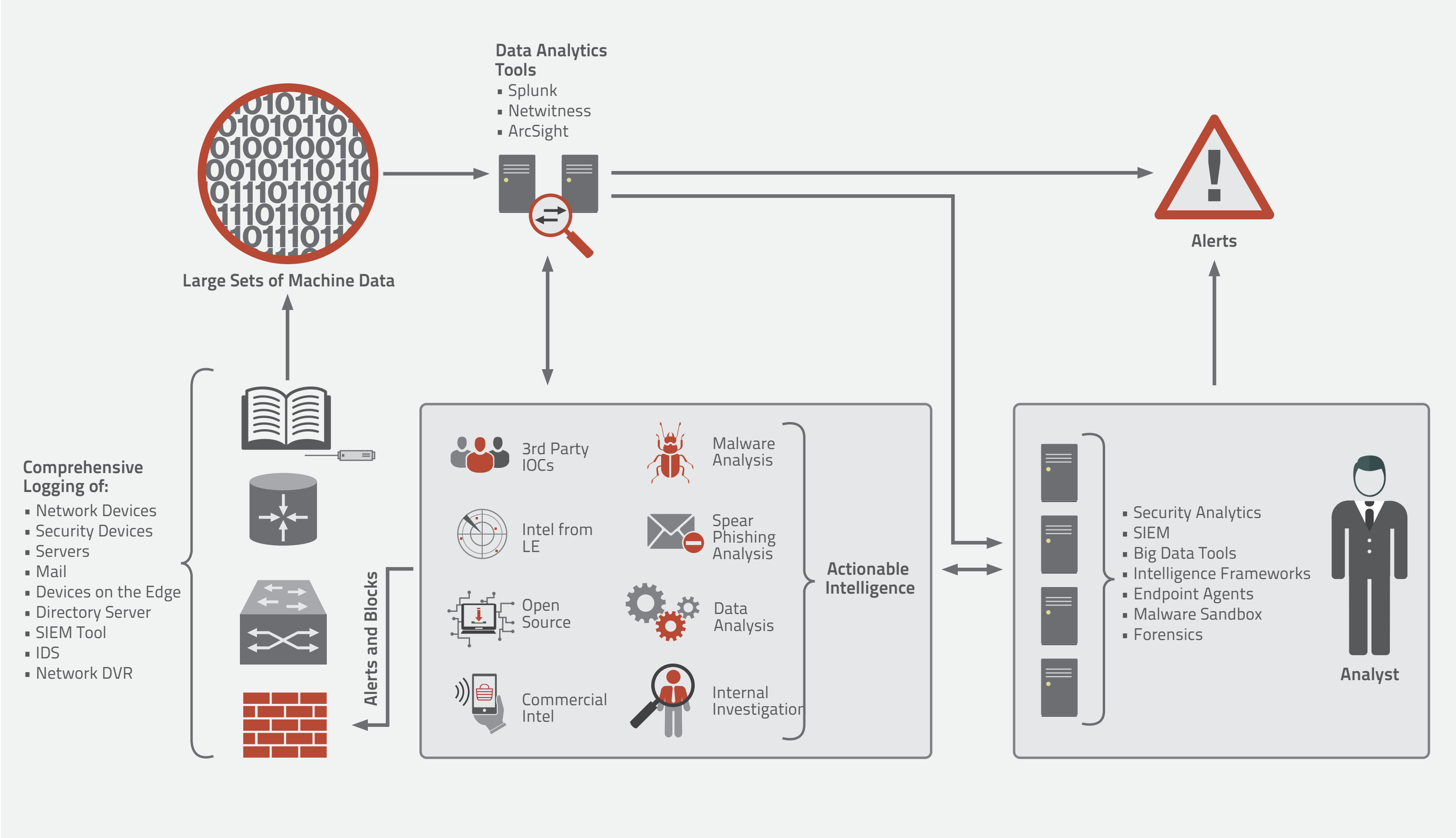
As the number of log sources grows, so does the volume of the log data being collected. This growth never follows a linear path. Each system generates more and more data; and with each system, another system comes into the scope. If all systems and devices are sending logs to a centralized system, which is the ultimate goal, the volume of data quickly becomes unmanageable.

With systems now producing more log data than ever before, and diverse data sources required to search out and locate a threat within the network, a new way to perform data analysis and identify correlated events is needed. The commercial SIEM companies are trying hard

(Continued on page 17)

Detecting Uninvited Guests

The full lifecycle tracks APTs across an enterprise, from robust logging and actionable intelligence to security analytics.



SOURCE: ADAM RICE

(Continued from page 15)

to play catch up and positioning their products to support the large volumes of data produced and collected.

ANALYTICS TOOLS

Big data analytics must provide the ability to correlate logging events based on time and user behavior across the entire spectrum of devices and technologies in an enterprise. Traditional SIEM tools are not good at this task because they organize data into databases, which become too big and clunky to query across. Typically, the flat files of machine data are best for fast queries. Several network tools designed for this purpose work very well. Splunk Enterprise and IBM QRadar Security Intelligence Platform are examples of big data analytics tools, but organizations need to build an integrated tool set that is designed to complement the security analyst's needs. With these tools and processes come unique skills. The evolving job of the modern security analyst is exactly what the big data problem needs.

With the right tools, a cybersecurity incident response team can follow the thread from a known event, like a malware alert, to behaviors of credentialed user accounts that are compromised, to machines from which the accounts are coming, to active IP sessions on the edge of the network. Without logging, none of this would be possible.

As CISOs build an active defense against the APT, the need to increase logging across the enterprise becomes a critical part of "seeing" and correlating events to track down the bad guys. It is not enough to simply turn on logging across the enterprise: People, tools and processes have to be established to use the data in a meaningful way.

Without a means of leveraging this big data quickly and dynamically, its usefulness disappears. Planning, process and skilled staff are all keys to using the large sets of machine data to win the battle against the APT. Before simply turning up logging across the enterprise, CISOs have to make sure that the budget is in place to acquire the big data analytics tools necessary to correlate events across the data, and that they have the staff with the expertise to use those tools. One without the other is not a workable solution. ■

ADAM RICE *is the CISO at Alliant Techsystems (ATK). An InfoSec professional with 17 years of experience, he has served as CSO of a global telecommunications company; general manager and vice president of a managed security services business; and director in several network consulting companies. He is a regular contributor to several information security publications.*

JAMES RINGOLD *is a senior enterprise security architect at ATK, who has worked in the aerospace and defense, electronic discovery and investigations and retail industries, performing technical evaluations and building information security programs in various stages. As a security operations manager and incident responder for 17 years, he focused on countermeasures and controls to detect and mitigate cyberintrusions.*

HOME

EDITOR'S DESK

DDoS DEFENSES

BIG DATA ANALYTICS

CISO TECH ASSESSMENTS

DATA SECURITY

A CHAT WITH DIANA KELLEY

SECURITY EDUCATION

Security Technology by the Numbers

Almost half of the security professionals surveyed ranked new security technology deployment as one of their top three initiatives.

Biggest Security Challenge

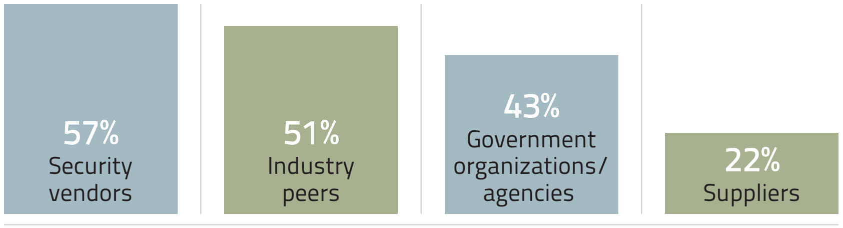
80%+

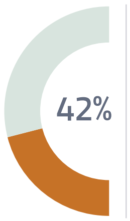
of the security professionals surveyed have seen the external threat increase in the past three years.

62%

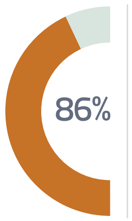
of respondents strongly agreed that the risk level to their organization was increasing due to the number of interactions and connections with customers, suppliers and partners.

Which external partners do you share threat information with?





of the organizations surveyed are members of a formal industry-related security group.



of respondents think industry-related security groups will become more necessary in the next three to five years.

SOURCE: 2014 IBM CHIEF INFORMATION SECURITY OFFICER ASSESSMENT, DEC. 2014; N=138 SECURITY PROFESSIONALS IN FIVE COUNTRIES

HOME

EDITOR'S DESK

DDoS DEFENSES

BIG DATA ANALYTICS

CISO TECH ASSESSMENTS

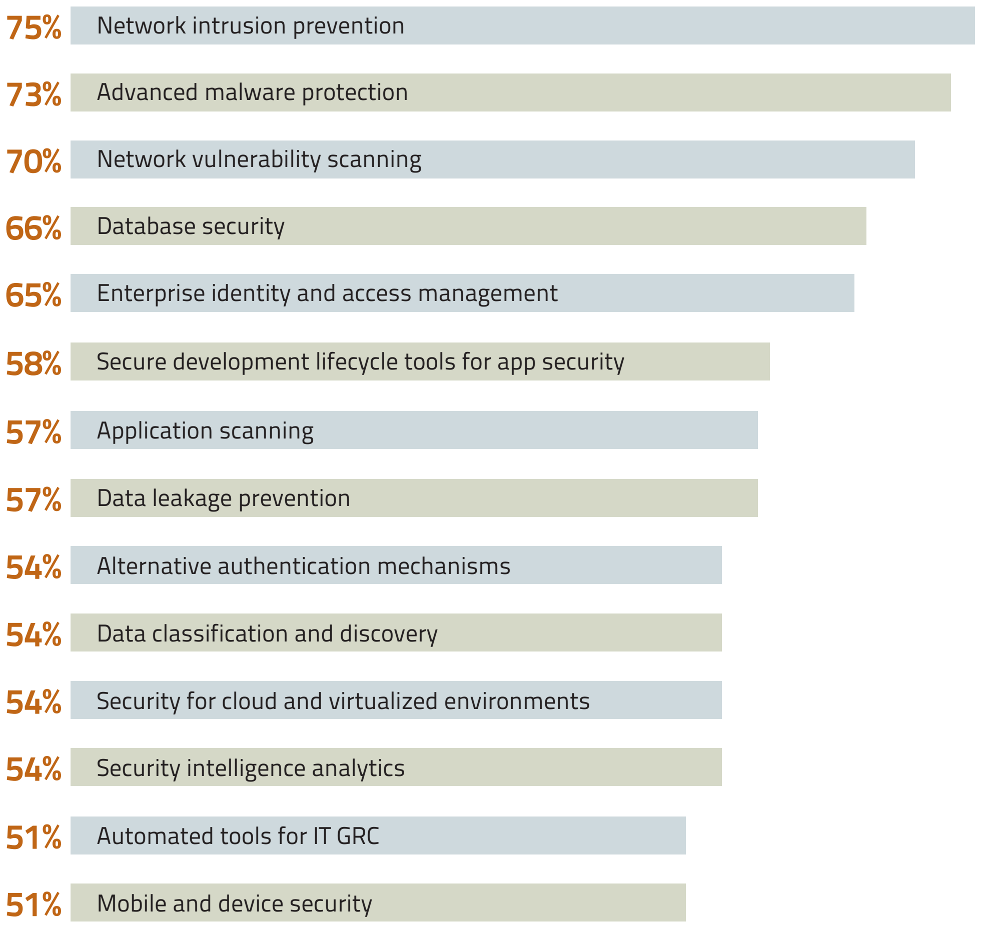
DATA SECURITY

A CHAT WITH DIANA KELLEY

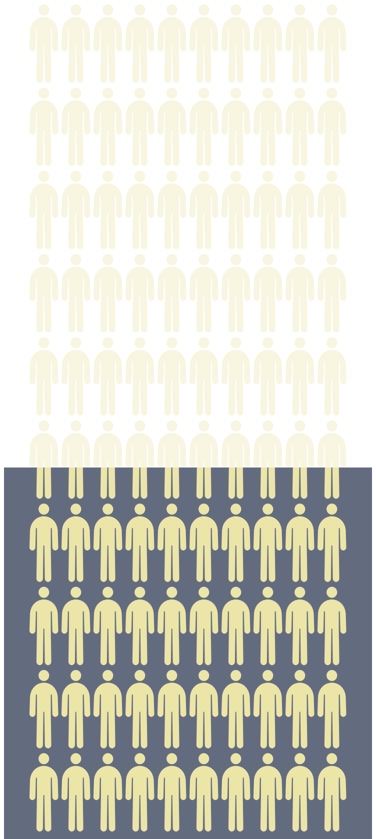
SECURITY EDUCATION

Security Technology Maturity

Would you rate the following technology in your organization as mature?



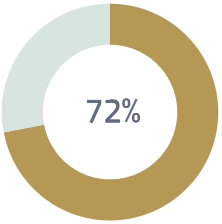
SOURCE: 2014 IBM CHIEF INFORMATION SECURITY OFFICER ASSESSMENT, DEC. 2014. N=138 SECURITY PROFESSIONALS IN FIVE COUNTRIES



ALMOST 50% of the security professionals surveyed ranked new security technology deployment as one of their top three initiatives.

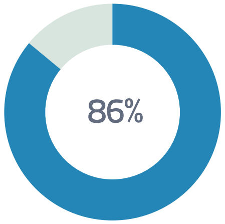
Current CISO Concerns

Data



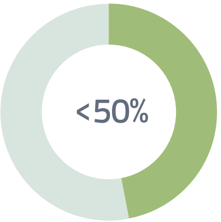
72% of security professionals said real-time security intelligence is increasingly important to their organization.

Cloud



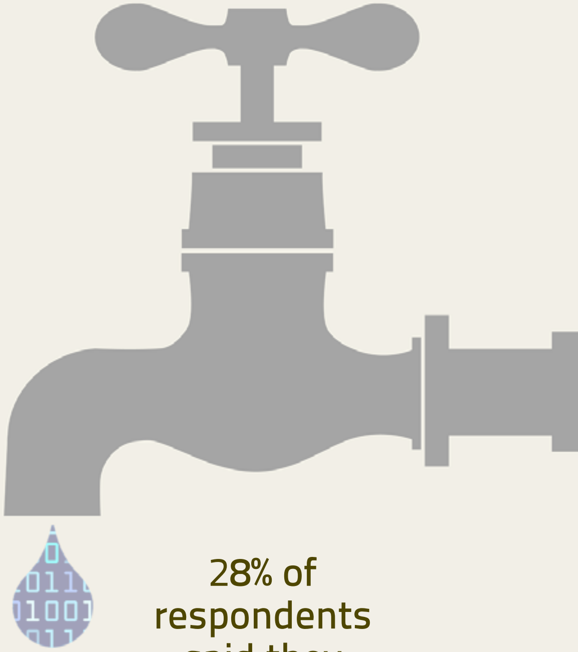
86% of respondents have either adopted cloud or are planning cloud initiatives. Three-quarters of those surveyed expect their cloud security budgets to increase or increase dramatically in the next three to five years.

Mobile



Less than 50% of security professionals believe they have an effective mobile device management approach.

SOURCE: 2014 IBM CHIEF INFORMATION SECURITY OFFICER ASSESSMENT, DEC. 2014
N=138 SECURITY PROFESSIONALS IN FIVE COUNTRIES



28% of respondents said they needed dramatic improvements in data leakage prevention, cloud and mobile security.

IMAGE SOURCE: THINKSTOCK

HEAT FROM THE BREACH

Enterprises re-ignite data classification and protection strategies after rocky 2014.

By Kathleen Richards

THE STEADY DRUM of high profile breaches continues to serve as a warning: In January, a financial advisor at Morgan Stanley allegedly stole 350,000 records about the firm's wealthiest clients and attempted to sell the data online. The Sony Pictures Entertainment hacking incident that played out over the holidays set many executives—already reeling from the risk and compliance ramifications of a year of unprecedented data security breaches—on high alert.

A *Wall Street Journal* reader poll in late December indicated that 54.3% of the respondents viewed the Sony, Target and Home Depot hacking incidents as the top compliance crisis in 2014, more than double the ranking of the Libor scandal, which had 22% of the vote. Moreover, 71.9% indicated that the issue expected to grow most in importance for their companies in 2015 was the combination of cybercrime and data privacy.

Although news of state-sponsored hackers may grab more of the headlines, it is insiders who are often behind the loss of intellectual property (IP) and other sensitive data. As often as not, these insiders don't realize their

HOME

EDITOR'S DESK

DDoS DEFENSES

BIG DATA ANALYTICS

CISO TECH ASSESSMENTS

DATA SECURITY

A CHAT WITH DIANA KELLEY

SECURITY EDUCATION

actions are a crime. A 2013 Symantec survey, conducted by the Ponemon Institute, showed that half of respondents admitted to taking corporate data when they left an employer and 40% indicated that they planned to use the data at a new job. More than half, 56% of those surveyed, did not view the transfer of IP for use at a new employer as a crime; 62% transferred corporate data to personal tablets, devices and cloud apps and never deleted the information. The survey resulted in three primary recommendations: educate employees, enforce non-disclosure agreements and implement monitoring technology in the form of data loss prevention (DLP) software.

DATA PROTECTION ON THE LINE

Jabil Circuit Inc., a global electronic services manufacturer headquartered in St. Petersburg, Fla., embarked on a DLP project in 2014 after hiring a new CISO the previous year. With 90 manufacturing plants and 180,000 dedicated employees in 23 countries, the company wanted to move from "low level" perimeter security to a tiered control set that could offer supply chain management and IP protection in line with customers' security requirements. Part of the challenge was a lack of standardization in footprint and technologies among Jabil's vastly different business units; the company packages and assembles electronics for telecommunications, healthcare, digital home, enterprise computing and storage, among other industries.

"We did a bunch of scans, and we brought in some consultants and did some assessments, and we realized that we had a lot of devices and a lot of endpoints and they were all at this low level of perimeter-based security—this one-size-fits-all security," Michael Ring, Jabil's senior IT manager, and threat intelligence and solution architect, explained during a presentation in November.

Jabil's security group is staffed with only about 30 people, and the global manufacturer has had a hard time finding the talent that it needed in the market that it serves. After hiring its new CISO, the electronics manufacturer embarked on several managed security projects and decided to contract with a DLP managed service provider, Digital Guardian (Verdasys), for greater visibility into endpoint data activity throughout the company, which includes cloud-based environments.

"We wanted … a tiered control set where we could provide the business units with the ability to choose—based on their customer mix and their requirements—a baseline level of security that met the company's policies," said Ring, "but also some higher levels that were more restrictive to give us more visibility around those assets and employees that were interacting with critical data."

Data classification for better IP protection played a role in the project. "We dove into what could be IP," he said. "We broke it into three categories: our pricing data, which is really our secret sauce; our PII, the employee

HOME

EDITOR'S DESK

DDoS DEFENSES

BIG DATA ANALYTICS

CISO TECH ASSESSMENTS

DATA SECURITY

A CHAT WITH DIANA KELLEY

SECURITY EDUCATION

data; and [what we] really focused on, which was the IP—our tool sets, our molds, customer plans and CAD drawings."

Deploying a DLP agent requires broad-based executive buy-in. The Jabil security team had adequate funding for the project, but they needed to get the CIO on board with the data protection strategy. "Really what got him there was that we had successfully deployed the Web proxy and SSO [single sign-on] services, and pivoted from existing tools as well, with no disruption to the business with immediate time to value," Ring said.

$300B

THE ESTIMATED AMOUNT OF REVENUE LOSS THROUGH IP THEFT, REPORTED BY THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY.

"Once we started paying those subscription costs, within a month we had [the DLP agents] covering the entire company, which is really rare for a large enterprise," he added. "The application-usage collection when you have this level of visibility was really interesting to [the CIO]; it helped us reconcile some software licenses, reduced some costs and saved us in some audit situations. It was without really controlling any data flow; it was just a side effect of having some visibility on the end point. "

During the DLP rollout, which took about 4 months and included a proof-of-concept stage with "friends and family," Jabil didn't report significant performance issues but did acknowledge a few problems with some applications. Visibility improved almost immediately, however, and the security team could see that data was getting copied to USB drives. "That was probably the real eye-opener to the executive management staff," said Ring. "No one really thought we had a data leakage problem. Once you put the agent out there, you get hard data right away that you have a data leakage problem. "

The manufacturer's security team used the egress reports from the DLP service to interact with the company's various business units at a high level. "You had over 10,000 documents moved from your customer shares on your core file server to USB; is that a work flow that you expected? That got some attention," Ring said. "That got some people from the business unit engaged and working with us to define what their workflows were, if there were USBs making sure that they were registered, if encryption was necessary due to sensitivity of data, if control was necessary. They are the ones that have to tell you that. So this got them to play ball."

CLASSIFICATION MATTERS

Data loss prevention technologies (network, endpoint and data discovery) can provide additional controls, such as notification and active blocking of valuable assets internally and at third-party sources, but context-aware tools require heavy lifting upfront, namely data classification and discovery. "Unless the company has an idea what it considers IP information, it makes it very difficult

HOME
EDITOR'S DESK
DDoS DEFENSES
BIG DATA ANALYTICS
CISO TECH ASSESSMENTS
DATA SECURITY
A CHAT WITH DIANA KELLEY
SECURITY EDUCATION

to make the most of the tools that are brought in," said Heidi Shey, analyst at Forrester Research. "IP is one of those tricky things where you really need a human to identify if something is considered intellectual property. It's not like a social security number where you can just write a regular expression for compliance."

Enterprises realize data classification is important, but for many it's something that gets put off because it is not easy to do or the company has tried before and failed.

"It takes effort and coordination across the enterprise. I think a lot of folks put it off to the side and address something sexier like mobile or cloud," said Shey. "But more and more, we are seeing that people are coming back around and realizing that they have to roll up their sleeves and tackle classification because they need to understand what data they have, and what is sensitive, if they want to do a better job—and focusing their efforts on protecting the sensitive information, and getting rid of stuff that they no longer need."

Enterprises looking at IP protection need to understand that any tool that you bring in, whether DLP or something else, is only going to look for data that has been identified and classified as sensitive or confidential by informed people, often within business units. DLP tools are increasingly offering user interfaces that are targeted at business users, who can work with IT to implement the policies and configure the tools so that the agents and alerts know what to look for.

> "IP is one of those tricky things where you really need a human to identify if something is considered intellectual property."
>
> *— Heidi Shey, Forrester Research analyst*

"With DLP, one of the mistakes that we see often is that people expect it to be magical," said Shey. "You bring it in; you turn it on and boom. But that is very far from reality, where so much more has to be done up front in terms of planning and considering policies that you have to implement and processes that you have in place to really enable these tools to work successfully."

Native installation on tablets and mobile devices is also an issue. Most content-aware DLP deployments still rely on mobile device management and VPN connections to scan traffic. Even so, enterprise interest in DLP as a control for IP protection is growing significantly—both for "soft" IP protection of things like text-based assets and process documentation and "hard" IP protection for CAD/CAM files, chemical formulas and source code, according to Gartner.

DLP managed services do not take away the headaches involved in creating content rules, policies and workflows, but may allow companies like Jabil to ramp up deployments more quickly by relying on the technical expertise and support of the service provider. While the managed services DLP market remains relatively small, Gartner estimates that 20% of DLP will be managed services by 2016.

LIMITED RECOURSE

Even with DLP controls in place, IP theft remains the elephant in the room for companies, dwarfing revenues lost by PII and other data security incidents. The losses are hard to quantify, but a 2013 report by the Commission on the Theft of American Intellectual Property estimated that it was upwards of $300 billion for U.S companies.

Once the theft has been discovered, what recourse does an organization have? Even with patents, and copyright and antipiracy laws in some countries, sometimes very little. Cyberinsurance does not cover losses associated with IP or trade secrets. Sony reached out to Mandiant, a division of FireEye and the FBI to help track down the perpetrators of the attack on their movie division. The company also hired a high-profile lawyer, David Bois, who sent a letter to media outlets threatening further action if they released stolen information.

While China has not been implicated in the Sony hacking incident, the country has been directly linked to other cybersecurity espionage and has continued to butt heads with the United States on IP issues. Companies that do business with partners in countries with lax data protection laws have limited recourse. It's critical to monitor and enforce security requirements through service level agreements and other contracts with third-party vendors and supply chains, such as Jabil.

Joint responsibility for data security, as well as rising awareness among C-level executives and boards, may drive renewed focus on data classification and better funding for IP protection. Data security is moving beyond IT at many companies; responsibility for IP protection often falls on chief privacy officers or data governance officers. "In the past, some of the mistakes that have been made with classification are that enterprises thought of it as a job for the security team and only the CISO," said Shey. "Someone in IT didn't think about business implications or that stakeholders should be involved, and that is changing today." ■

KATHLEEN RICHARDS *is the features editor of* Information Security *magazine. Follow her on Twitter* @RichardsKath.

The Metrics Dilemma

Measurements do not always answer the hard questions, but you can take steps to improve the process, says IBM's executive security advisor.

BY MARCUS J. RANUM

M**ETRICS THAT GET** results have proved challenging for many security teams. In addition to figuring out what to measure, security professionals have to know which measurements and analytics their organization's executives and board actually care about, and many CISOs falter at this step.

Diana Kelley knows how to build a successful metrics program. As the executive security advisor to IBM Security Systems, she leverages 25 years of IT security experience to provide advice and guidance to CISOs and security professionals. Kelley has contributed to the IBM X-Force report and frequently publishes on the company's Security Intelligence and Smarter Planet blogs. She is also a faculty member with IANS Research and serves on the advisory board for InfoSec World 2015 and the IBM Network Science Research Center Smart Grid Advisory Group. Marcus Ranum talked with Kelley—a former SearchSecurity.com contributor—about security metrics, risk appetite, and short and long term ways that security professionals can improve their metrics efforts.

MARCUS RANUM: It seems that metrics are one of the areas where computer security practitioners have trouble getting traction. Why do you think that is? And what's your first suggestion for how an organization can get started with a metrics program?

I suppose I loaded that question when I said 'metrics program.' Do we even need a specific metrics effort or is there some other approach to getting a clue of what's going on?

DIANA KELLEY: My first suggestion is to figure out what the organization wants to achieve with the metrics, because that will inform what needs to be measured as part of the metrics and analytics program, or even if the company wants or needs a metrics program. Measurements are fairly simple: How many high sev vulns [severe vulnerabilities] are there in our public-facing websites? Or, even, how many public-facing websites do we have?

Metrics compare or analyze the measurements to get to some answer. For example: We had seven high sev vulns last week, five high sev vulns yesterday and 10 today, so what does that tell us about the state of the public websites? Getting deeper into the analytics—kind of public-facing app, language or stack, and development team can all be added to the mix—to turn the measurements into metrics. But there's no point gathering all that data if it's answering a question no one at the company cares about. And sometimes companies want answers that they just can't get the measures for, such as 'Am I safer today?'

It's important to remember that different roles and groups will care about different metrics. An auditor will be focused on metrics related to compliance while a CIO may care more about performance and improvement.

I've been pretty notoriously dismissive of risk management on the basis that it's 'garbage in, garbage out,' and I finally realized that the real problem is that we, as an industry, don't have a good way of generalizing the outputs from our metrics (or we don't keep them at all). How can, say, a bank produce useful security metrics that a hospital might be able to consume? Are metrics always an inward-facing process, or is there a useful way of sharing our experiences?

Risk management in the classic—determine the risk LxI (likelihood x impact) and then decide the organization's risk appetite for each risk, and then figure out what controls and processes need to be in place to contain the risk at the approved risk level? Do you see 'garbage in, garbage out' because LxI are so hard to quantify and calculate? Or is it that there are just too many risks to consider to do this well? Because those are the big hurdles I see companies dealing with in risk management.

The other big one is asking the IT team to set risk appetite. IT's role is to present risk calculations to the business; then the board needs to figure out the risk appetite. But very often the business wants IT to set appetite. Another messy area is translating IT risk into business risk.

I believe there are many metrics that can be useful across verticals, but they'd be part of the overall metrics and risk program. Each individual organization then needs to understand what it wants to do with those metrics. To make that less abstract, consider something like a series of DDoS attacks coming from specific IP addresses that are targeting the bank. These IP addresses are bots or shadow sites. Although the health system isn't being

HOME

EDITOR'S DESK

DDoS DEFENSES

BIG DATA ANALYTICS

CISO TECH ASSESSMENTS

DATA SECURITY

A CHAT WITH DIANA KELLEY

SECURITY EDUCATION

'DDoSed' by those IP addresses yet, it may want to be proactive and block those IP addresses or work with a DDoS prevention company that gathers IP reputation information from across verticals to do the blocking for them.

On the other hand, if the bank is looking at risks related to transactional latency in the milliseconds, those measures may have less importance to a health system that can tolerate a second of transactional latency.

Alex Hutton likes to say his favorite metric to ask for is 'What are my riskiest business units?' What do you think of that? I'm sort of leery of the idea that one organization's metrics might work for others or for everyone. Do you favor organization-specific metrics or more 'meta' ones?

Well, first of all, I think Alex Hutton [director of operations, risk and governance at a financial institution] is wonderful, and anyone that hasn't heard him talk about risk and metrics needs to get to one of his talks as soon as possible. The question, 'What are my riskiest business units?' is fantastic, but incomplete. Because, again, we need to get back to whether or not LxI have been calculated properly and for the right risks. And then the organization needs to ascertain the [risk] appetite for the business units. I've spoken to an organization that did a cost-benefit analysis of PCI compliance or taking the hit of fines and a failed return on compliance. They went with taking the hit. That's a very 'personal' decision that the company made for risk acceptance. Most organizations would say being non-compliant to PCI is very risky—but that company didn't.

Diana Kelley

That's why I agree with you about being leery of one-size-fits-all metrics. Many standard measurements have value across verticals (days to patch), but what that means for risk at each company will vary by type of device—is the unpatched system a medical device that needs to be re-certified if it's patched, or a website?—and risk requirements of the organization.

Where I think it all comes down is that simple measures can be meta but turning those into risk metrics (LxI) and appetite need to be unique to the vertical and specific organization. One of the big problems is organizations want an easy answer, but risk metrics and analytics aren't easy.

Another issue we haven't touched on yet is misinterpreting the numbers. I did a piece on this for IBM's Security Intelligence blog a while back. Sometimes we look at stats that seem to indicate 'people are living longer' and want that to mean we can all be the non-ape version of the fifth Earl of Gonister in Aldous Huxley's *After Many*

HOME

EDITOR'S DESK

DDoS DEFENSES

BIG DATA ANALYTICS

CISO TECH ASSESSMENTS

DATA SECURITY

A CHAT WITH DIANA KELLEY

SECURITY EDUCATION

a Summer. But dig a little on that data and it turns out we're not living much longer, we're just better at not dying younger.

Is your company truly at a lower risk level because patches are applied more quickly? Or are you just unpatched for a smaller amount of time, but now suffering more outages due to buggy patches? It's tricky.

Like you say, it's amazingly tricky. One of the things that drives me nuts about all this is that you can have an axis to the problem, which you haven't considered, and when you slice the data across that axis, a whole new reality falls out. For example, we might notice that longevity in the U.S. has gone up slightly, but if we slice the longevity across wealth, we discover that the wealthy are doing much, much better. They are pulling the average for everyone up, while some sectors are actually doing worse. This makes me extremely leery when I see a large complex metric that amounts to a roll-up of accumulated information: Sometimes, it reveals; sometimes, it obscures.

Exactly! Dependencies that weren't accounted for, like wealth in longevity, can change the analysis and 'answers' significantly. Also, I do think sometimes people influence what they are looking for and the results they want to see. Risk calculations should be pretty cold and objective; risk appetite decisions can be much more subjective. But cold and logical doesn't always work for people. I'm thinking of Fight Club and how the company Ed Norton's character works for only cares about cost to pay off families of the dead and injured people and to deal with the PR fallout versus cost to recall all the cars. That's horrifying but if cash outlay is the biggest risk, it makes sense. In IT risk, many companies make the personal interpretation that employees are more trustworthy and it's the outsiders from a foreign country that are the bigger risk. But data doesn't prove that out.

I love reading Paul Krugman's Economics and Politics blog on NYTimes.com because he's really delightful at explanatory metrics; whether you agree with him or not about meta-economic theories, he sure explains his position well.

That's a great point—regular reading of Paul Krugman's blog could help IT risk [professionals] a lot because he shows how to explain complex models and analysis in a clear way.

I worry that people's understanding of big data is that it is some kind of magical thing that's going to figure out their data for them, whereas I see it mostly as an exploratory tool. It's like a friend of mine once said about his Hong Kong tailor: He can make you the best suit that you know how to ask for.

HOME

EDITOR'S DESK

DDoS DEFENSES

BIG DATA ANALYTICS

CISO TECH ASSESSMENTS

DATA SECURITY

A CHAT WITH DIANA KELLEY

SECURITY EDUCATION

What's been the most successful use of metrics you've seen in a business context?

Ha! That's a perfect analogy for big data. If you don't know what you're looking for, how do you know you're gathering the right data? In the measure-everything approach (which is a good one) the problem shifts to how do you know you're writing the right analysis rules to find risk-related information? One kind of cool thing about big data is that we can look for patterns and see if those relate to causality and get better with rules over time. At least big data is an attempt to gather and measure everything that we haven't seen before.

Short-term activities can be as simple as looking for the patient-zero laptop or device where re-infection of malware originates—maybe that device is syncing to an infected one when it's off the corporate network—or looking for high levels of failed logins. such as brute force attacks or a restrictive password aging policy that's frustrating users.

Long-term advanced analytics could get us to a much better understanding of how risk evolves in an organization. Tracking employee reviews could reveal that employees who get bad reviews are more likely to go rogue and try to steal data or perform other malicious activities. Or that certain seemingly unrelated attack patterns—like ping sweeps followed by a rash of negative comments on Twitter or Facebook and an increase in phishing emails—mean the company's been targeted and needs to tune alert-response levels.

IT risk metrics and analytics are tough and imperfect right now. But if we don't get started looking for at least a few answers, we're not going to figure out what we're doing wrong or missing, and won't be able to get to a better place. Actuarial tables adjust as new dependencies and risk factors are uncovered. They're not perfect, but they're good enough to keep most big insurance companies in business. IT risk metrics may never be pinpoint perfect—is anything?—but we can definitely do better. ■

MARCUS J. RANUM, *chief security officer of Tenable Security Inc., is a world-renowned expert on security system design and implementation. He is the inventor of the first commercial bastion host firewall.*

Planting Cybersecurity Seeds for the Future

SMU's Frederick Chang says the shortage of trained staff is inhibiting enterprises' ability to defend their networks. His cybersecurity program is designed to address the skills gap.

BY FREDERICK R. CHANG

A**N ANCIENT PROVERB** tells us, "The best time to plant a tree was 20 years ago. The second best time is now." In many ways this saying captures the essence of our work in cybersecurity at Southern Methodist University (SMU). Let me comment briefly on our two most important priorities—research and education—and how we are investing in the future.

At SMU we've recently formed the Darwin Deason Institute for Cyber Security and in our research at the Institute, we're working to advance the development of the science of cybersecurity. After decades of computer security research, in practice too many companies still find themselves in a "penetrate and patch" predicament—a situation that is far too ad hoc and after-the-fact.

Whether it's through increased systematic experimentation, more powerful empirical models or theories with greater explanatory power and more, increasingly, there's a recognition that we need better answers to cybersecurity-related questions: What can we measure? What can we predict? What can we replicate? What can we prove?

In the battle against human disease and injury, physicians and health care professionals benefit from the deeper understanding made available from medical science. Similarly, system designers and information technology professionals could more effectively combat security-related challenges with better laws, principles and fundamentals that would result from cybersecurity science. It is becoming increasingly urgent that security be built into our cybersystems with the scientific understanding and engineering discipline that's required in building bridges, skyscrapers, rail lines, water systems and other critical physical infrastructure.

Research is needed that will produce insights and generalizations that are independent of any particular software, system, network, vulnerability or attack. The existing research base has certainly produced important findings and many of these findings have been put into practice, but a coherent science of security does not yet exist—and it will take a long time to create it. With the help of many outstanding students, we're working at SMU to contribute to that science, and we think it is important to take a broad, interdisciplinary approach in doing so.

On top of the many technical, business, policy and process issues that information security professionals must address today, over the past several years there has been a widening skills-gap problem: There simply aren't enough trained cybersecurity people to fill today's need. The shortage of trained staff is inhibiting our ability to defend enterprise networks and systems adequately. Some estimates indicate that there may be as many as 1 million job openings globally for information security professionals. Job postings increased 74% from 2007 to 2013—a growth rate two times faster than for all information technology jobs, according to one report. In 2013 there were over 200,000 information security job openings in the U.S. alone. A cybersecurity report issued by the U.K.'s National Audit Office in 2013 noted that the skills gap there could take up to 20 years to address.

At SMU we take seriously our responsibility to help train today's millennials so that they can contribute immediately upon graduation. One key advance we've implemented in the current academic year is that we now require our bachelor of science students in computer science and computer engineering to take a foundational cybersecurity course as part of the core curriculum.

> We now require our bachelor of science students in computer science and computer engineering to take a foundational cybersecurity course as part of the core curriculum.

At a minimum these students will gain a much deeper appreciation for the field and will be better able to protect themselves in cyberspace. More importantly, this required course may inspire some students to take more advanced courses and pursue a career in cybersecurity upon graduation or continue their education with graduate training in the field.

Enrollment of new computer science majors has gone up across the country over the past several years, and that—combined with an increasing number of information security classes—should help to whittle away at the skills-gap problem. That said, I believe we need to reach out beyond computer science majors. Going forward, it will be important to offer a broader survey course that will appeal to a much wider audience of students on our campus. In an effort to increase the size of the population that might eventually pursue a career in cybersecurity, I also have begun making plans to reach out to a K-12 student audience in Dallas this year.

Despite the challenging cybersecurity landscape that we face today, I remain optimistic about the future. That optimism is based in large part on my interaction with the students on our campus, and knowing that a good number of them will become cyber defenders in the years ahead. Creating a science of cybersecurity and closing the skills gap will take some time, but we must be patient and invest in the future. It's time to plant a few seeds. ■

FREDERICK R. CHANG *is at SMU (Southern Methodist University, Dallas) where he is Bobby B. Lyle Endowed Centennial Distinguished Chair in Cyber Security, director of the Darwin Deason Institute for Cyber Security, professor in the Lyle School of Engineering and a senior fellow in the Tower Center for Political Studies. He spent many years in the private sector and is the former director of research at the National Security Agency. Dr. Chang has been awarded the National Security Agency Director's Distinguished Service Medal. He has served as a member of the Commission on Cyber Security for the 44th Presidency, and as a member of the Computer Science and Telecommunications Board of the National Academies.*

TechTarget

TechTarget Security Media Group

EDITORIAL DIRECTOR Robert Richardson

FEATURES EDITOR Kathleen Richards

EXECUTIVE MANAGING EDITOR Kara Gattine

ASSOCIATE MANAGING EDITOR Brenda L. Horrigan

EXECUTIVE EDITOR Eric Parizo

SITE EDITOR Robert Wright

DIRECTOR OF ONLINE DESIGN Linda Koury

COLUMNISTS Marcus Ranum, Pete Lindstrom

CONTRIBUTING EDITORS Kevin Beaver, Crystal Bedell, Mike Chapple, Michele Chubirka, Michael Cobb, Scott Crawford, Peter Giannoulis, Francoise Gilbert, Joseph Granneman, Ernest N. Hayden, David Jacobs, Nick Lewis, Kevin McDonald, Sandra Kay Miller, Ed Moyle, Lisa Phifer, Ben Rothke, Mike Rothman, Karen Scarfone, Dave Shackleford, Joel Snyder, Steven Weil, Ravila Helen White, Lenny Zeltser

VICE PRESIDENT/GROUP PUBLISHER Doug Olender
dolender@techtarget.com

TechTarget
275 Grove Street,
Newton, MA 02466
www.techtarget.com

About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

COVER IMAGE AND PAGE 4: TANG YAU HOONG/GETTY IMAGES