Managing the Insider Threat

New Challenges for Today's Organizations

May 2016

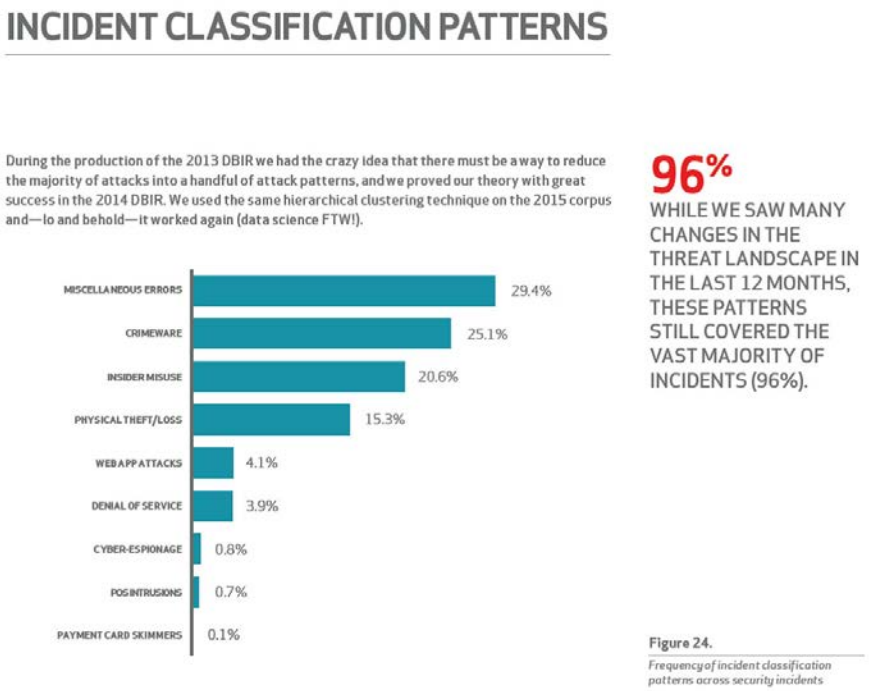
By Brad Gow, Senior Vice President, Endurance Insurance

Advisen
Transforming • Insurance™

Today's companies are under siege from malicious actors seeking to compromise their networks in order to steal intellectual property and sensitive customer and employee information.

Perpetrators range widely. On the high end, sophisticated state-sponsored intelligence gathering organizations and organized cybercriminals target specific intellectual property and sensitive employee records for later exploitation. On the lower end, cashiers and service staff surreptitiously swipe customer credit cards through portable readers hidden in jackets or under skirts. But regardless of whether the threat originates externally or within a company's staff, information breaches almost always involve some failure on the part of authorized network users. Whether malicious or simply acting out of carelessness or ignorance, individuals with daily access to a company's network are the most difficult aspect of information security for an organization to manage.

According to the 2015 Verizon Data Breach Investigation Report, the top four attack patterns – Miscellaneous Errors, Crimeware, Insider Misuse and Physical Theft/Loss – all involved authorized network users. [1]



[1] 2015 Verizon Data Breach Investigations Report, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf, (2015).

In addition to often crippling financial and reputational damage, victimized organizations also face unprecedented fines and penalties from state and federal government agencies. In April, 2015 the Federal Communications Commission (FCC) fined AT&T $25 million for failing to protect customers' information after employees were found to have stolen and sold names, addresses and social security numbers. This is the largest FCC fine levied to date. [2]

However, there is an upside. While employees can be careless, irrational and naive, they can also be trained to be the first line of defense in protecting an organization from network based attacks. While defensive tactics won't prevent employees from losing laptops with sensitive information or intentionally stealing intellectual property, training can raise awareness and alert employees to potential threats.

Each of these threats – malicious colleagues and sophisticated outsiders preying on employee carelessness or ignorance – has its own defining characteristics and presents its own challenges.

Malicious Employees

Over the past three years, cyber espionage – principally by state actors – has reached crisis proportions, affecting all sectors of American business at a staggering cost. According to a McAfee study the annual economic costs of cybercrime in the US range from $20 billion to $120 billion, the majority a result of the wholesale theft of design patents, copyrights and other intellectual property. [3]

One of the worst nightmares for any chief executive of an organization reliant on intellectual property for a competitive advantage is the theft of that information. Employees who are greedy, disgruntled or simply subscribe to lofty ideals are often in a position to access and distribute sensitive information. While several have become household names – Edward Snowden and Bradley Manning, as examples – the vast majority of thefts never make the headlines.

An extreme example of employee cyberespionage is AMSC, a Massachusetts-based company that supports the wind turbine industry with generators, drivetrains, systems and software. American Superconductor (as it was originally known) had an extensive trading relationship with Sinovel, a Chinese-based manufacturer of wind turbines with

[2] Ruiz, R. Rebecca, "F.C.C. Fines AT&T $25 Million for Privacy Breach," NYTimes.com, http://bits.blogs.nytimes.com/2015/04/08/f-c-c-fines-att-25-million-for-privacy-breach/?_r=1, (April 8, 2015).

[3] The Center for Strategic and International Studies and McAfee, *"The Economic Impact of Cybercrime and Cyber Espionage,"* mcafee.com, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf,(June 2013).

a worldwide customer base. Sinovel depended on AMSC for the complex software used to regulate the flow of generated electricity from the turbine to the electrical grid.

In March 2011, Sinovel abruptly stopped accepting shipments from AMSC, who maintained $100 million in accounts receivable and another $700 million in outstanding orders from what had been to that point their biggest client. Later that year, while working on a turbine in China, AMSC engineers discovered a version of their Low Voltage Ride Through (LVRT) software on a Sinovel turbine despite the fact that AMSC had never sold or licensed the technology to Sinovel.

In the following weeks, AMSC's suspicions centered on a high level engineer, Dejan Karabasevic, who had abruptly resigned the same month Sinovel broke off the corporate relationship. An investigation revealed extensive email and Skype communications between Karabasevic and Sinovel executives, including a plot for Karabasevic to abscond with AMSC's software and modify it for use in Sinovel equipment. For his role in the theft, Karabasevic was offered $1.7 million as well as a Sinovel-supplied apartment in Beijing.

Karabasevic was ultimately charged with corporate espionage, but the damage to AMSC was severe. Revenues fell from $286 million in fiscal 2011 to $76 million a year later, while the stock price fell from $336 to $43 over roughly the same period. Today AMSC's stock price sits under $10 per share.

Industries which are heavily dependent on product innovation are particularly at risk from unscrupulous employees stealing research and development results for resale to a competitor. Federal prosecutors recently indicted five individuals, including two research scientists, who had been employed by British drug maker GlaxoSmithKline (GSK) on charges that they had stolen confidential research data on cancer drugs with the intent to sell the information to competitors in China. [4] In January 2016 Yu Xue, a biotechnology researcher in Pennsylvania, and Lucy Xi, another GSK scientist, were charged with conspiracy to steal trade secrets, conspiracy to commit wire fraud, conspiracy to commit money laundering, theft of trade secrets and wire fraud after downloading and emailing research data to a company they set up in China that would have allowed buyers to easily replicate a dozen or more GSK formularies. This ongoing case should serve as a wakeup call to the pharmaceutical, technology and other industries heavily reliant on R&D for a competitive advantage.

[4] Berkret, Bill, "Five charged in U.S. with stealing secrets from GlaxoSmithKline," Reuters.com, http://www.reuters.com/article/us-glaxosmithkline-indictments-idUSKCN0UY2V2, (January 21, 2016).

Innocent Employee Errors

While malicious insiders can wreak havoc, the financial impact of their exploits to US businesses is dwarfed by the everyday errors of innocent employees.

Maintaining a secure network environment is a constant challenge for Chief Information Security Officers and their staff, and one that continues to become more difficult by the day. Hundreds of hours and millions of dollars spent constructing strong perimeter security can be rendered useless by a single careless employee clicking on an infected website or inadvertently opening a phishing email.

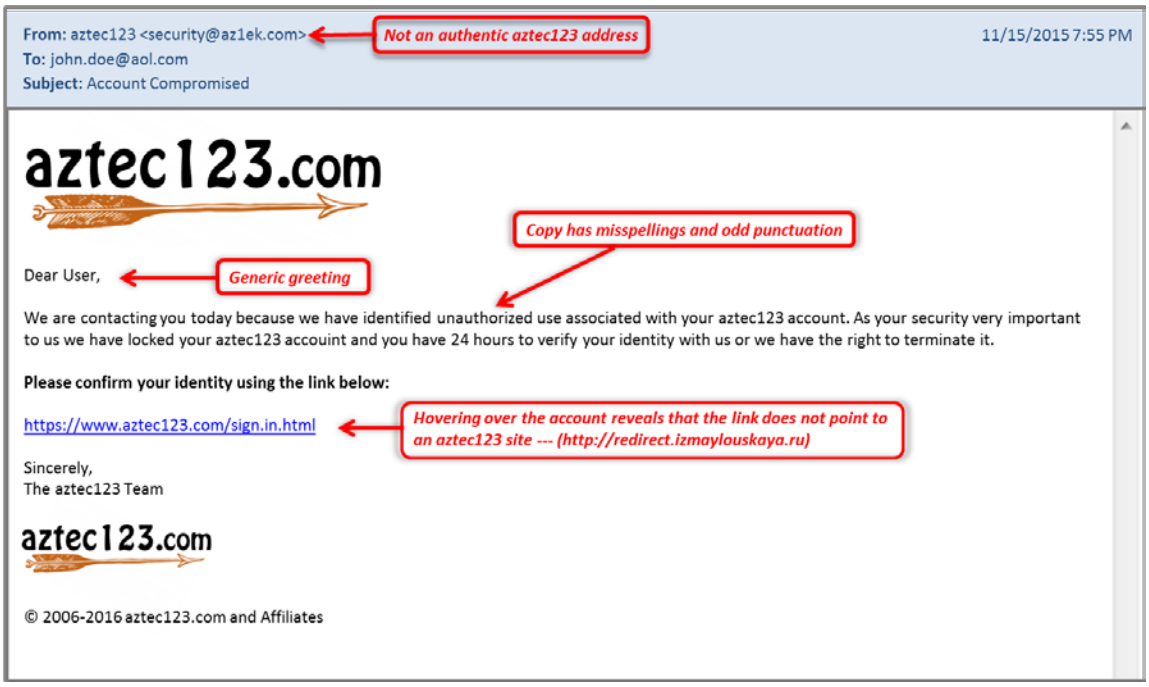
According to Ernst & Young's 2015 Global Information Security Survey, the top two threats today are phishing and malware…both inextricably linked to careless or inattentive employees. Other threats include social engineering fraud and the surge in unauthorized use of cloud services.[5]

Where in the past a 'security by obscurity' strategy may have been sufficient for smaller companies to stay under the radar, it is no longer the case. Cybercriminals have grown extremely sophisticated in their ability to specifically target and monetize a compromised network regardless of the target company's size, and are now compiling malware which automatically spreads itself to any network meeting the malware author's desired characteristics.

Phishing

Wikipedia defines phishing as "the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication."
This exploit has been with us for years, initially as '419' scams referring to the section of the Nigerian penal code addressing fraud schemes. While few targets are still willing to arrange wire transfers to Lagos in exchange for a share of a prince's fortune, phishing attacks have grown increasingly sophisticated, luring even trained users to provide sensitive personal or corporate information. Attackers are getting better at masking email addresses and URLs and carefully copying branding and crafting language to fool even vigilant employees.

[5] Ernst & Young's 2015 Global Information Security Survey, "Creating Trust in the Digital World," http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf, (2015).



Malware

Today, the most imminent threat IT administrators face is email infected with malware that allows hackers to gain a toehold inside a corporate network. In one scheme as clever as it is dangerous, hackers steal GPS data and email addresses from mobile phones, then send spoofed emails purportedly from the local police department notifying victims of a speeding ticket. The emails accurately reflect times, street names and speeds driven…only when the hyperlinked image of the driver's license plate is clicked is malware loaded onto the email recipient's computer.

A recent phenomenon has been the proliferation of so-called ransomware, malware typically introduced to a corporate network by an employee clicking on an infected link which results in the instant encryption of a user's computer or server with an algorithm effectively freezing out the user. The victim is typically instructed to send bitcoin – an untraceable digital currency – in order to receive the key enabling them to decrypt their own data. This exploit has been fabulously successful, with an estimated tens of thousands of paying victims over just the past year. Accurate estimates are difficult to come by due to the relatively low demands made – typically $500 - $20,000 per incident – and the embarrassment factor which typically prevents victims from coming forward.

The first quarter of 2016 saw multiple hospitals affected by ransomware, including Hollywood Presbyterian Medical Center in California and Henderson, Kentucky's Methodist Hospital. Interestingly, there appears to be little correlation between the ransoms requested and the size of the target organization. Hollywood Presbyterian, while a little more than double the capacity of their Kentucky counterpart, was asked for $3.6 million while Methodist Hospital was offered the key to decrypt their own data for only four bitcoin or $1,600. Interestingly, the Hollywood Presbyterian hackers settled for only $17,000 or 40 bitcoin, likely to cut short negotiations before investigators could identify them. [6]

Social Engineering Fraud

Most people are naturally cooperative and helpful – a trait that scammers abuse to trick individuals into compromising either information or money. Funds transfer fraud targets companies which work with foreign suppliers and regularly wire funds internationally. Usually beginning with a phishing exploit to compromise a corporate email account, attackers identify senior managers and employees in an organization who have the ability to carry out wire transfers. Millions of dollars have been stolen by attackers impersonating senior managers with a realistic corporate email ordering Accounts Payable or other departments to urgently prepare and execute a wire transfer.

Ubiquity, a San Jose based manufacturer of wireless technology products, fell victim to a scheme whereby internal communications were compromised and fraudulent funds transfer instructions were sent to the finance department of a Hong Kong subsidiary. According to SEC filing in June 2015, a total of $46.7 million was transferred from the subsidiary to overseas accounts held by third parties before they were detected. Only about $8.1 million has been recovered to date.[7]

According to a FBI Public Service Announcement dated August 2015, total Business Email Compromise (BEC) losses from October 2013 through August 2015 totaled over $1.2 billion, with the majority impacting victims in the U.S. The same report also cited a 270% increase in BEC scams since January of last year, indicating that the threat and effectiveness of these scams are growing exponentially. [8]

---

[6] "Ransomware hackers steal a hospital. Again.," http://boingboing.net/2016/03/25/ransomware-hackers-steal-a-hos.html, BoingBoing.net, (March 25, 2016).

[7] SEC Filing, i.e., Ubiquity, Networks, Inc., https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm, (Form 8-K) (August 4, 2015).

[8] FBI Public Service Announcement, http://www.ic3.gov/media/2015/150827-1.aspx#fn2, (August 2015).

Unauthorized Resource Usage

While phishing, malware and social engineering schemes dominate the headlines, there are myriad avenues for employees to compromise corporate networks and information. Network administrators frequently identify data leakage through insecure portals, including peer-to-peer file sharing, unauthorized remote access tools and now more commonly misuse of cloud computing resources.

According to recent information from Cisco Systems, Chief Information Officers estimate that their organizations use an average of 91 distinct cloud computing services. [9]This may be low by a factor of ten - Cisco estimates that the average organization's employees are using 1,120 cloud based services via their corporate network. This 'Shadow IT', as it is known, comprises a broad range of services from social networking, music and entertainment sites to cloud-based data processing and storage sites like Microsoft Azure and DropBox. The storage of corporate information on external facilities, often unknown to IT management, can lead to the compromise of personal information or corporate secrets.

The use of cloud-based storage services can also facilitate the exfiltration of corporate secrets by unscrupulous staff. Moving R&D data, customer lists or other proprietary data into a Google Drive or DropBox account to access later is easy, mostly invisible to IT staff, and no doubt is happening every day across corporate America.

Risk Management's Response to New Challenges

While unprecedented computing power allows employees to boost productivity and efficiency, it also multiplies potential damages. Unfortunately, Moore's Law doesn't apply to corporate risk management practices which are significantly lagging these new threats to corporate reputations and balance sheets.

There is no silver bullet to eliminate or even significantly reduce the exposure presented by malicious insiders; however, there are a number of steps that organizations are taking to reduce the insider threat.

Awareness and Training

Increasing employee's overall awareness of systems and information security is the best way to ingrain security into an organization's culture. This is primarily

[9] Clark, Don, "Cisco Reports Rapid Rise of Unauthorized Cloud Storage,"www.wsj.com, (January 13, 2016).

accomplished by periodic training in the tenets of information security. This includes recognizing information that should be considered confidential and establishing unambiguous expectations in terms of individual responsibility for maintaining a secure environment, including recognizing and reporting potential data breaches and other threats.

Web-based information security training is broadly available and should be a requirement for new employees and for periodic review by all staff. Some companies go a step farther and test staff by sending carefully crafted phishing messages. Those that fall prey to the message by clicking on an offending link are mandated to attend further training. A number of organizations which handle massive amounts of personally identifiable information (PII) hold annual 'security weeks' to remind staff of the importance of operational information security. Others implement information security hot lines where employees can confidentially report potential concerns or breaches to senior management.

Network Monitoring Tools

Dozens of software tools are available that allow system administrators to monitor and analyze network traffic for patterns suggesting misuse and to identify and block the exfiltration of sensitive information (e.g. social security numbers in an email) from the network. Periodic network and security log reviews should be standard practice. Companies are now adopting other more sophisticated tools which readily allow them to monitor website browsing, individual user keystrokes, and third party cloud usage by their employees. While it will always be difficult to identify an IT-savvy employee intentionally looking to steal corporate information or misuse corporate system resources, having the right monitoring tools in place augments periodic system log reviews to uncover malicious activity.

Psycholinguistic Tools

While network monitoring tools can alert IT security staff to suspicious activity after it has occurred, a new breed of enterprise-level tools proactively monitor communications over a period of time to gauge individual employee sentiment and identify individuals at risk of 'going rogue'. This new technology enables companies to take appropriate measures to proactively prevent potential sabotage or espionage on the network.

* * *

Managing the threat of malicious insiders and employee errors is a challenge for any organization, but it is not insurmountable. A formal employee training program, with ancillary initiatives to maintain employee awareness can contribute to a culture of security. Technical controls and monitoring tools can further augment privacy and security training and awareness.

Creating the proper information security culture is not solely IT's responsibility…it is a multidisciplinary endeavor that should include Legal, Human Resources and IT, and needs to be visibly supported by executive leadership to be successful.