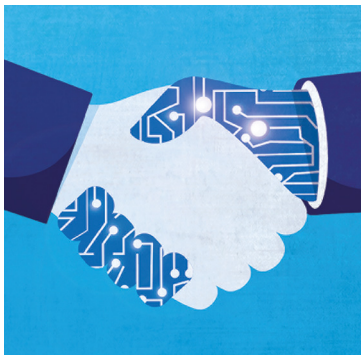
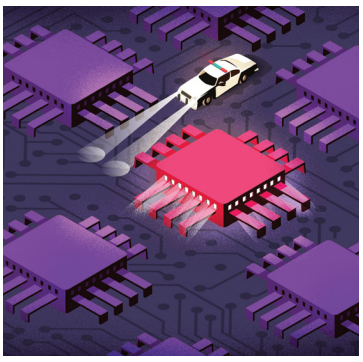
SECURITY MANAGEMENT

Powered by ASIS INTERNATIONAL
Advancing Security Worldwide®

Securing Your Organization's Most Vulnerable Asset: Information

This collection of articles from the security profession's premier publication takes a look at the variety of ways your organization's information assets are at risk and what your security function should do about it.





SECURITY MANAGEMENT

Spies in the Supply Chain

A major compromise of the cybersecurity supply chain shows how network intrusions into a single entity can have thousands of victims.

By Megan Gates

Not all security incidents are created equal. They don't all get the attention of the CEO. But one in the fall of 2020 did. Cybersecurity firm FireEye received a notification through its internal systems that an employee had registered a second device to access corporate networks.

It seemed odd. So, CEO Kevin Mandia was briefed and the security team followed up with the employee to ask him if he had registered an alternative device to access the work network. He said no, and FireEye launched an investigation—discovering that someone else had bypassed FireEye's two-factor authentication system to register the device, gain access to FireEye's systems,

and make off with the company's Red Team tools.

But how did the hacker get in? To find out, FireEye conducted a thorough analysis of its systems and identified that the point of earliest compromise occurred in spring 2020 from a system connected to Orion business software, a product it had purchased from the firm So-

And FireEye was not SolarWinds' only high-profile customer. It also did business with numerous U.S. federal government departments and agencies, telecommunications firms, Fortune 500 companies, and many others.

larWinds, Mandia said in an Aspen Institute briefing on the breach.

FireEye ultimately decided to reverse engineer SolarWinds' software, and discovered that Orion itself had been compromised. Hackers had infiltrated the software supply chain, compromising the SolarWinds system to covertly gain access to its customers' systems.

"After an initial dormant period of up to two weeks, [the attack method] retrieves and executes commands, called 'Jobs,' that include the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services," according to FireEye's blog about the breach. "The malware masquerades its network traffic as the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files, allowing it to blend in with legitimate SolarWinds activity. The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers."

And FireEye was not SolarWinds' only high-profile customer. It also did business with numerous U.S. federal

government departments and agencies, telecommunications firms, Fortune 500 companies, and many others.

FireEye's decision to disclose then set off a mad dash among other SolarWinds customers to determine if they also had been compromised. The U.S. Cybersecurity and Infrastructure Security Agency (CISA), part of the U.S. Department of Homeland Security, issued an emergency directive requiring U.S. government agencies to take a variety of actions, including disconnecting or powering down SolarWinds Orion products on their networks. "SolarWinds is so prevalent it's almost like what Kleenex is to tissues," said Jake Williams, an analyst and senior instructor at the SANS Institute, as well as founder of Rendition InfoSec, in a SANS webinar held shortly after the disclosure. "They are one of if not the de facto network management system with 300,000 plus customers."

SolarWinds' position as a network management system (NMS) made it a lucrative target for infiltrating other networks because it could communicate with devices it was managing or monitoring on customers' networks, Williams explained.

The sophistication of the infiltration also made it nearly impossible for customers to detect and was the work of a threat actor with the "resources, patience, and expertise to gain access to and privileges over highly sensitive information if left unchecked," CISA said in a statement.

The agency would later join the FBI, the Office of the Director of National Intelligence, and the National Security Agency (NSA) in a task force dubbed the Cyber Unified Coordination Group to investigate and remediate the incident. In a statement, the task force attributed the SolarWinds breach to Russia as part of

an intelligence gathering effort affecting approximately 18,000 public and private sector SolarWinds customers, including multiple U.S. government agencies.

Russia has denied any involvement in the breach of SolarWinds and subsequent infiltration of government and corporate networks. In an interview with Russian news agency TASS, Kremlin spokesman Dmitry Peskov said, "any accusations of Russia's involvement are absolutely baseless, they are more likely to be a continuation of blind Russophobia that is resorted to in case of any incident."

Countries spy on each other, but the volume and level in term of governmental entities and private sector enterprises...ought to be alarming to all of us.

While initial concerns pointed to the possibility that the hackers could use their access to disrupt their victims' networks, many in the U.S. government have called it an act of espionage to further intelligence gathering efforts.

Speaking in an Aspen Institute panel in January 2021, U.S. Senator Mark Warner (D-VA), incoming chair of the U.S. Senate Intelligence Committee, said Americans need to be concerned about the ability of a nation-state actor to intrude into government and private sector networks.

Warner also added that the intrusion was spurring conversation about whether it was "within the bounds of acceptable espionage? Countries spy on each other, but the volume and level in terms of governmental entities and private sector enterprises...ought to be alarming to all of us."

While the scope of the SolarWinds infiltration may be unique, the number of cyber-espionage attacks is on the rise, says John Grim, senior manager of investigative response at Verizon and lead author of Verizon's inaugural Cyber-Espionage Report published in fall of 2020. The report analyzed data collected for Verizon's annual Data Breach Investigations Report (DBIR) to assess the state of cyber-espionage across the globe and within public and private sectors.

The analysis found that generally the education, finance, information, manufacturing, mining and utilities, and public sectors were hardest hit by cyber-espionage. Threat actors—most (85 percent) associated with a nation-state—also managed to compromise their targets within seconds to days through a variety of techniques, such as backdoors (91 percent), phishing (90 percent), downloaders (89 percent), and more. And once inside, threat actors would linger—often for months, as seen in the SolarWinds compromise of FireEye—to exfiltrate data from their victims and risk detection.

"In the real world—by extension the cyber world—it's a challenge to detect. These threat actors are after data that is sensitive and proprietary," Grim says, adding that many successful cyber-espionage breaches are not reported because they may remain undetected or may not be required to be disclosed because they did not compromise personally identifiable information.

Threat actors who engage in espionage also work to fly under the radar or blend in by using the tools of the network environment, such as IT administrative rights, Grim explains.

To help address the increasing number—and potential severity—of cyber-espionage intrusions, Warner advocated for an accounting of incidents and an es-

tablishment of norms. He praised FireEye's Mandia for his commitment to disclosing the breach and providing details to help security practitioners better protect their systems. But Warner cautioned that relying on the "goodwill and patriotism" of CEOs was not enough—rules and policies are needed to require disclosures.

Also at the Aspen Institute panel, Katie Moussouris, founder and CEO of Luta Security, added that while the idea of creating norms in cybersecurity for espionage and weapons is popular, those involved are hesitant to take options off the table.

"The idea of setting norms feels to me like we're in the decline of the digital Roman Empire and we're trying to tell people it's not okay to use elephants to cross the Alps," she says. "Meanwhile, [the adversary] is using elephants to cross the Alps and we will be overrun."

Moussouris also said that instead of focusing on limiting the use of a specific technology or the development of a weapon, any regulations and norms should focus on behaviors and use case scenarios.

"It's not the technology that needs to be under these norms, it's the behavior we need to enact to preserve the world order in general," she added.

In the meantime, there are actions that security practitioners can take to limit the threat and increase their ability to detect intruders in their systems. This begins, Grim says, with assessing the most valuable data, the safeguards surrounding that data, and the tools and people with access to that data.

Grim also recommends vetting third party entities and having written agreements in place about the security provisions related to such parties.

"Monitor their access into your environment and, at least annually, review your written agreements," he

says. “So, when we get more into the applications that may be provided from an outside entity, we’re making sure they are fulfilling their obligations.”

Williams made similar suggestions in the SANS webinar, adding that these types of intrusions are extremely difficult to detect, and sometimes the best course of action is to have a robust response plan.

For organizations compromised by the SolarWinds hack, “I’m willing to say that unless they were doing some nasty stuff in your environment this was not something that most of us were going to prevent,” Williams said. “If I ran SolarWinds in my environment, I would have been compromised as well.”

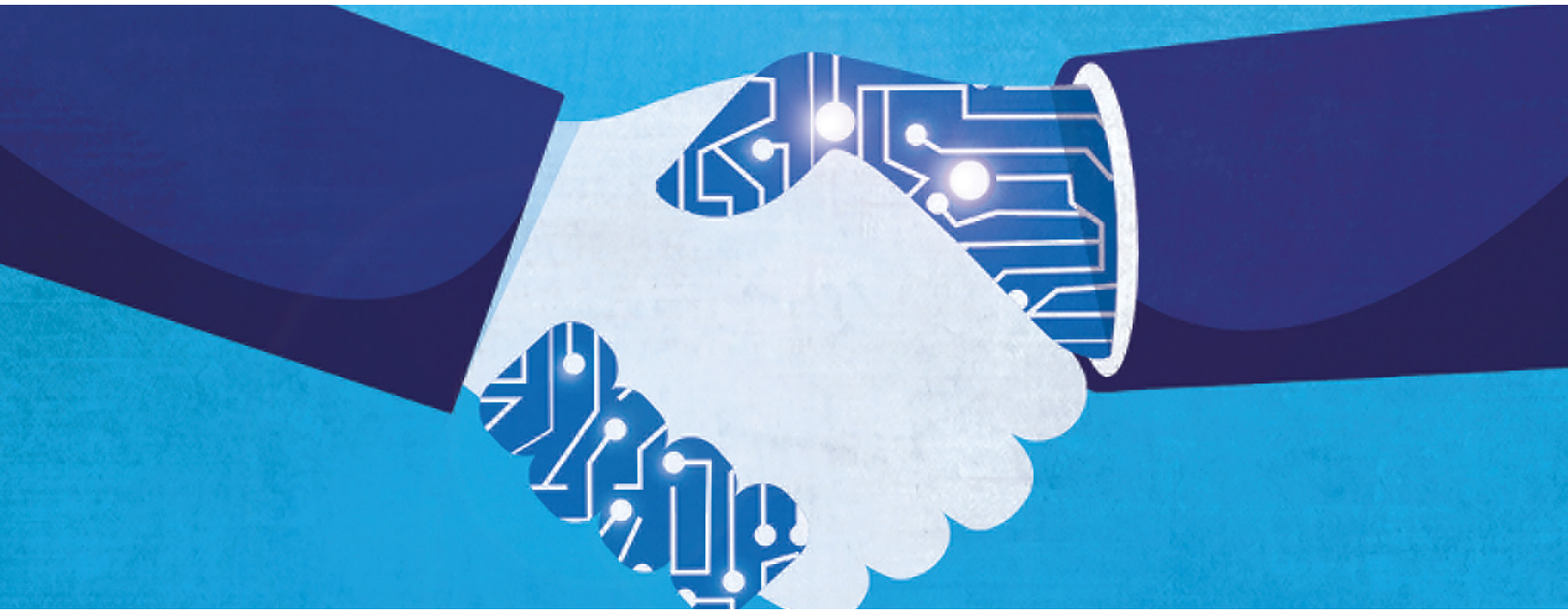
MEGAN GATES IS SENIOR EDITOR AT SECURITY MANAGEMENT. CONNECT WITH HER AT MEGAN.GATES@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @MGNGATES.

SECURITY MANAGEMENT

The Deal with Due Diligence

After a major decline in mergers and acquisitions due to the COVID-19 pandemic, businesses are increasingly interested in pursuing deals. And cybersecurity is taking center stage.

By Megan Gates



It was a deal that made Marriott International the owner of the largest hotel chain in the world. In 2015, the company announced that it would buy Starwood Hotels & Resorts Worldwide, Inc., for $12.2 billion—combining the two companies' 5,500 hotels with 1.1 million rooms worldwide.

But unbeknownst to Marriott, the deal would open up a massive area of liability just a few years down the road when the U.S. Federal Trade Commission (FTC) would fine Marriott for a breach of Starwood's guest reserva-

tion database—which exposed the personal information of up to 500 million people.

"The hotel chain says the breach began in 2014 and anyone who made a reservation at a Starwood property on or before September 10, 2018, could be affected," according to the FTC's announcement.

Marriot later clarified in an update in 2019 that approximately 383 million guest records were compromised in the breach—including 20.3 million encrypted passport numbers and 5.25 million unencrypted passport numbers.

Along with the fine from the FTC, the hotel owner was also fined more than £99 million ($130 million) by the United Kingdom's Information Commissioner's Office for the breach; the commissioner's office has since reduced the fine to £18.4 million ($25 million) because of the COVID-19 pandemic.

Additionally, Marriott has faced a slew of legal complaints related to its handling of the breach. One of the largest is a class action lawsuit brought by two members of Starwood's—and now Marriott's—customer loyalty program on behalf of all victims of the breach.

"It is particularly egregious that Marriott did not discover this serious data breach during the course of its due diligence efforts in conjunction with its 2016 Starwood acquisition," said Amy Keller, partner at DiCello Levitt and co-lead counsel on the suit. "Marriott seems to forget that part of being in the customer service business includes actually taking care of its customers. Through this lawsuit, we intend to ensure that it never forgets that again."

And while those efforts are focused on ensuring that Marriott learns from previous mistakes, recent findings from a Deloitte survey suggest that organizations are

taking cybersecurity more seriously during the merger and acquisition (M&A) process—especially when those deals are being made virtually.

In the Future of M&A Trends Survey of 1,000 U.S. corporate merger and acquisition executives and private

It is particularly egregious that Marriott did not discover this serious data breach during the course of its due diligence.

equity firm professionals, Deloitte found that deal activity in the United States plunged after the World Health Organization declared COVID-19 a pandemic in March 2020. But in April 2020, the situation changed with 60 percent of respondents saying their organizations were more focused on pursuing new deals. Six in 10 survey respondents also said they expected U.S. merger and acquisition activity to return to pre-COVID-19 levels within the next 12 months.

"When it comes to cyber in an M&A world—it's important to develop cyber threat profiles of prospective targets and portfolio companies to determine the risks," said Deborah Golden, cyber and strategic risk leader, Deloitte. "CISOs understand how a data breach can negatively impact the valuation and the underlying deal structure itself. Leaving cyber out of that risk picture may lead to not only brand and reputational risk, but also significant and unaccounted remediation costs."

In practice, this means that organizations are increasingly giving CISOs a seat at the table and making them part of the due diligence process, says Jaime Fox, part-

ner and principal at Deloitte Cyber Risk Services. Fox leads Deloitte's work on cyber due diligence in strategic acquisitions.

Previously, security representatives were only brought into the deal-making process during the closing aspects so they could focus on integrating the organizations involved, she says. Taking that approach, however, means that organizations might not discover a cyber risk—like the Starwood data breach—before finalizing the deal, opening themselves up to potential liability, higher remediation costs, and more consequences down the line.

Initially, organizations began to transition their approach to cyber due diligence by doing a high-level cybersecurity assessment. This included aspects like looking at a broad threat landscape and overall network security, Fox explains. Before the COVID-19 pandemic hit in early 2020, clients were requesting that cyber be more fully addressed in due diligence.

"Now in a COVID world, we're seeing deeper dives into what clients are looking at," she adds. "We see acquirers doing things in terms of threat intelligence and research on the Dark Web to gain a greater understanding around things like leaked user credentials for sale. It's very encouraging to see…and helps the CISO frame the mind-set: 'This is the house I'm about to buy. These are the things I've uncovered. This is what my remediation costs are going to be.'"

These deep dives include creating a cyber playbook that defines the areas the parties want to cover in their due diligence process, including threat intelligence, Dark Web research, cyber reconnaissance, and assessments of network flows to identify potentially suspicious traffic. Some also choose to engage in penetration testing.

"Oftentimes the target will approve doing something like that—sometimes they won't," Fox says. "It's very encouraging to see clients and acquirers push to get this type of information. It really helps to home in on their top 10 questions—after they've gathered this intelligence, they can go to the target and gain a better understanding of what they've found."

This was on display, for instance, when Verizon reduced its offer to acquire Yahoo! by $350 million after Yahoo! disclosed two major breaches. And the portion of Yahoo! that was not part of the Verizon deal agreed to assume 50 percent of the liability related to any future lawsuits stemming from the breaches, according to analysis from PricewaterhouseCoopers (PwC), When Cyber Threatens M&A.

"This isn't an issue for only tech companies. Cyber threats have spread to industries that weren't targeted earlier in the digital age; restaurant chains, for example, can be attacked for the customer information—either credit card numbers or information from their loyalty programs," PwC said. "Furthermore, the goal of a cyberattack can be more than a simple data grab. Consider a pharmaceutical company's formula for a drug, a manufacturer's product design, or a distribution company's transportation model. All of that is intellectual property that can be a crucial part of a deal's value."

These threats raise the risks for acquirers looking to make a deal—and make their potential acquisitions a more lucrative target during the integration process—but do not tend to push them away from the table.

"While cyber threats are more prevalent, it's still rare for a breach or other issue to harm a transaction to the point that an acquirer completely walks away; delaying the transaction is a more common result," according to

PwC. "Yet delays, added costs, and questions about a target's value all have consequences for the deal process. To avoid such damage, acquirers need to understand the cyber risks of the target so they can limit surprises, model appropriately, and ensure a reasonable transaction."

This is key, Fox adds, because discovering this information sooner in the process will allow acquirers to negotiate better terms.

"Right off the bat we tell our clients that going through this process sooner is only going to help you in the end," she says. "Understanding the impact of security breaches, controls around customer data, and arming them with information around how it's important to understand the entity you're about to buy…when you present it from a risk perspective, you show that these are things we should be able to quantify."

There's also a renewed focus on cybersecurity as many of the mergers and acquisitions happening today are being done virtually. Eighty-seven percent of respondents to Deloitte's survey said their organizations have effectively managed a deal in a purely virtual environment, and more than 55 percent said they anticipate virtual deal-making will be the preferred platform even after the pandemic.

MEGAN GATES IS SENIOR EDITOR AT SECURITY MANAGEMENT. CONNECT WITH HER AT MEGAN.GATES@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @MGNGATES.

SECURITY
MANAGEMENT

An Unfair Advantage

The United States is facing an unprecedented wave of attempts to obtain intellectual property and trade secrets. Nearly all of them are coming from China.

By Megan Gates

Hongjin Tan had a good job. A Chinese national and U.S. legal permanent resident, he was employed as an associate scientist for a U.S. petroleum company to work with a team developing the next generation of battery technologies for stationary energy storage.

But after just over two years at the company, Tan contacted his supervisor on 12 December 2018 to give his two weeks' notice. Tan said he wanted to return to China because, as an only child, he needed to be there to care for his aging parents. He did not have a job lined up back home but was in negotiations with a few battery companies about a position.

After Tan gave his notice, the company—following security procedures—revoked his access to company sys-

tems and reviewed his recent computer activity. What it found was concerning.

Tan had accessed hundreds of corporate files, including reports on how to make a specific product and the plans to market that product in China. The information was considered a trade secret and outside the data Tan needed access to for his job. The review also found that Tan downloaded restricted files outside of his scope of work to a personal thumb drive, without authorization.

Later that same evening, Tan texted his former supervisor, admitting that he had a USB drive with lab data on it that he had been planning to write a report on from his home.

The company escorted Tan from the property after the review and banned him from returning. Later that same evening, Tan texted his former supervisor, admitting that he had a USB drive with lab data on it that he had been planning to write a report on from his home. He was asked to return the drive, which he did. The drive contained research documents that had significant value for the company and were marked as confidential and restricted.

The next evening, Tan went to dinner with a former colleague and confessed that on a trip to China in September 2018 he had interviewed at a Chinese company and been in constant contact with company officials. The company, based in Xiamen, had developed production lines for different battery materials.

The former coworker reported the conversation to the company, which reached out to the FBI to report a theft of trade secrets. The Bureau analyzed the corporate laptop Tan had been using and found a letter from the

company in Xiamen dated 15 October 2018. The letter confirmed that Tan would be the energy new material engineering center director at the company, as long as he guaranteed that information he had provided and would provide in the future was "real and effective."

The FBI has more than 1,000 intellectual property (IP) theft cases open involving individuals associated with the People's Republic of China.

Tan was charged with the theft of a trade secret, unauthorized transmission of a trade secret, and unauthorized possession of a trade secret. He later pled guilty to the charges and was sentenced to 24 months in a U.S. federal prison for stealing information worth more than $1 billion.

"American companies invest heavily in advanced research and cutting-edge technology. Trade secret theft is detrimental to our national security and free-market economy," said Melissa Godbold, special agent in charge of the FBI Oklahoma City Field Office—which handled Tan's case. "It takes profits away from companies and jobs away from hardworking Americans. The sentencing of Hongjin Tan underscores the FBI's commitment to protecting our country's industries from adversaries who attempt to steal valuable proprietary information."

While the facts of Tan's case are unsettling, they are not entirely unusual. The FBI has more than 1,000 intellectual property (IP) theft cases open involving individuals associated with the People's Republic of China. And those thefts have cost the United States nearly $500

billion a year, says William Evanina, director of the National Counterintelligence and Security Center (NCSC).

"We've never seen the likes of economic espionage that we've seen in the past 24 months," he explains. "And a majority of that has come from the Communist Party of China."

CHINA'S RISE

Prior to the coronavirus pandemic, China's economy was growing rapidly—a trend that had continued for years, making its economy second only to that of the United States.

The expansion of China's economy followed the opening of the country in the 1980s and the growth of its middle class. The Chinese Communist Party also laid out strategic goals for the groundwork that would allow it to one day take a dominant position in producing advanced technologies to ensure its national security and global economic position.

To achieve these goals, China invested in human capital, infrastructure, and research within its own borders and abroad. It became a major investor in technology firms and promoted research and study at foreign institutions. China also weakened internal regulatory barriers for businesses—which allowed domestic firms to flourish—along with creating subsidies to build national champions.

"China's leaders want to move away from a dependence on foreign technology, so that China moves up the production value chain and is no longer just the assembler of other nations' intellectual property," wrote James Lewis, senior vice president and director of the Center for Strategic and International Studies' (CSIS) Technology Policy Program, in an analysis of China's economic

and trade practices. “Since the 1980s, China has sought to build a strong technology base and has made repeated efforts to achieve this. The primary motivation is to enhance China’s security and national power.”

A prime example of this is China’s aviation sector, which originally relied on Soviet-based manufacturers. When China opened its economy, other nations moved to partner with China to produce a better-quality product.

“Part of the requirement imposed on them for market access was coproduction, where Chinese aviation companies worked with Western aircraft firms to make parts for Western commercial aircraft or help assemble

While much of China’s ability to acquire technology and intellectual property was done through foreign direct investment, it also has carried out a broad cyber espionage campaign—beginning in the 2000s and continuing today.

them,” Lewis explained. “Coproduction, over 20 years, taught Chinese companies essential production know-how, and the quality of Chinese aircraft has improved markedly.”

This improvement, in turn, might encourage the Chinese government to pressure domestic airlines to buy these Chinese-made products while also imposing barriers for foreign firms to compete in its market.

“Chinese policy is to extract technologies from Western companies; use subsidies and nontariff barriers to competition to build national champions; and then create a protected domestic market for these champions to give them an advantage as they compete globally,” Lewis explained in his research. “Huawei is the best exam-

ple of a globally dominant Chinese company built along these lines, but there are others. A senior Chinese official once remarked that if China had not blocked Google from the China market, there would be no Baidu," one of the largest Internet and AI companies in the world.

While much of China's ability to acquire technology and intellectual property was done through foreign direct investment, it also has carried out a broad cyber espionage campaign—beginning in the 2000s and continuing today.

"The Chinese discovered that the Internet gave them unparalleled access to poorly secured Western networks," Lewis explained. "Cyber espionage is accompanied by collection efforts by human agents, both in China and in other countries, but the most rewarding collection programs have shifted from human agents targeting Western facilities located in China to cyber espionage."

China has also engaged in a campaign of commercial espionage, targeting Western companies at an extremely high rate.

"They're not just targeting defense sector companies," said FBI Director Christopher Wray at the U.S. Department of Justice's China Initiative Conference in February 2020. "The Chinese have targeted companies producing everything from proprietary rice and corn seeds to software for wind turbines to high-end medical devices. And they're not just targeting innovation and R&D. They're going after cost and pricing information, internal strategy documents, bulk [personally identifiable information (PII)]—anything that can give them a competitive advantage."

One example is the massive Equifax breach that compromised data on nearly every American and several

thousand Canadians. Along with the charges of violating the Computer Fraud and Abuse Act, the U.S. Department of Justice also charged four members of China's People's Liberation Army (PLA) with trade secret theft for allegedly acquiring Equifax's data compilations and database designs.

"Unfortunately, the Equifax hack fits a disturbing and unacceptable pattern of state-sponsored computer intrusions and thefts by China and its citizens that have targeted personally identifiable information, trade secrets, and other confidential information," said U.S. Attorney General William Barr in a statement.

China has repeatedly denied that it was involved in any way in the Equifax breach and data theft. China's Foreign Ministry Spokesman Geng Shuang told the Associated Press that China is committed to "firmly oppose and combat cyberattacks of any kind" and that its institutions "never engage in cybertheft of trade secrets."

According to the U.S. intelligence community and the FBI, China has also targeted hospitals and research institutions to obtain insights into their work and provide it to domestic institutions. In a virtual conference hosted by the Aspen Institute in April 2020, FBI Cyber Division Deputy Assistant Director Tonya Ugoretz said the Bureau has seen increased reconnaissance and cyber intrusions of the U.S. healthcare sector and research institutions to gain insight into how they are addressing the coronavirus pandemic—especially organizations that have made announcements about their COVID-19 research.

"There are certainly good reasons for those institutions to tout the work they're doing and educate the public on the work they are doing," Ugoretz said. "The sad flip side is that it kind of makes them a mark for other na-

tion-states that are interested in gleaning details about what exactly they're doing—and maybe even stealing proprietary information those institutions have."

This type of activity did not begin as the coronavirus was spreading, but has been occurring for some time, Evanina says, and is related to China's Thousand Talents Plan. The plan, issued in 2008, incentivizes individuals engaged in research and development in the United States to provide that knowledge to China in exchange for salaries, research funding, lab space, and more, according to a U.S. Senate Homeland Security report.

Recently, the former chair of Harvard University's Chemistry and Chemical Biology Department, Dr. Charles Lieber, was arrested and charged with making a false statement to law enforcement when he allegedly lied about being involved with the Thousand Talents Plan.

In his role at Harvard, Lieber received more than $15 million in grant funding from the National Institutes of Health and the U.S. Department of Defense for his research into nanoscience. The grant funding required him to disclose significant foreign financial conflicts of interest, such as funding from foreign governments.

"Under the terms of Lieber's three-year Thousand Talents contract, Wuhan University of Technology (WUT) paid Lieber $50,000 per month, living expenses of up to 1 million Chinese Yuan, and awarded him more than $1.5 million to establish a research lab at WUT," according to the U.S. Department of Justice (DOJ). "In return, Lieber was obligated to work for WUT 'not less than nine months a year' by 'declaring international cooperation projects, cultivating young teachers and PhD students, organizing international conference[s], applying for patents, and publishing articles in the name of' WUT."

Lieber allegedly told investigators in 2018 that he was

not asked to participate in the Thousand Talents Program, but he was unable to say how China categorized his work, according to the DOJ.

These kinds of partnerships, intrusions, and thefts show that while China is interested in obtaining intellectual property and trade secrets, it also needs to understand the business process to be able to use them.

"It does little good to steal intellectual property if you do not have the expertise to use it, and until recently, this was true for much of China's espionage in advanced technology," Lewis explained. "What has changed in the last decades is that China has realized that acquiring 'know-how' is more important than acquiring IP. In many cases, China now has the money and the skill to use much of the IP it has acquired licitly or illicitly."

MITIGATING THE THREAT

While China's ability to acquire intellectual property and trade secret information is concerning for its economic impact, it also has ramifications for its adversaries' national security.

In its 2020–2022 national strategy, the NCSC included countering the exploitation of the U.S. economy as one of its strategic pillars.

"Adversaries use front companies, joint ventures, mergers and acquisitions, foreign direct investment, and talent recruitment programs to gain access to and exploit U.S. technology and intellectual property," the strategy said. "They also influence and exploit U.S. economic and fiscal policies and trade relationships."

While costing Americans billions of dollars, this transfer of knowledge "harms U.S. economic, technological, and military advantage in the world," the strategy explained. "It puts at risk U.S. innovation and the com-

petitiveness of American companies in world markets."

And that activity is not limited to the United States alone; members of the NATO alliance are seeing similar attempts by China to acquire intellectual property and business processes, particularly in the energy sector, says Evanina, who also acts as the chair of counterintelligence for NATO.

One of the major challenges in mitigating the threat, however, was a lack of awareness from the private sector about China's activity.

"China is stealing their stuff—not our stuff," Evanina tells Security Management. "We need to provide information to allow CEOs to make risk-based decisions based on our strategy."

To help raise awareness, the NCSC began partnering with academic associations and U.S. Senators Richard Burr and Mark Warner to conduct briefings with college and university presidents.

"We brought in 150 university presidents and gave them a classified briefing," Evanina says. "And the FBI provided the opportunity for them to see classified cases, strategic plans by the Chinese to educate them about the threat."

The NCSC has used a similar approach to briefings with CEOs, CISOs, and CSOs. So far, Evanina estimates that they have reached 14,000 executives in the private sector where the NCSC laid out the economic impact of China's activities.

Providing this information and insight is critical, Evanina adds, because the U.S. government historically has not done the best job explaining the threat in a way that allows institutions to take action to mitigate it.

During these briefings, leaders are instructed to identify what it is their organization makes or sells that is

critical to the sustainability of their company, create mechanisms to protect those assets, share the protective steps with stakeholders, and build internal employee support for protecting corporate assets.

Evanina says the briefings also focus on encouraging organizations to enhance their overall security posture and encouraging them to create insider threat programs.

"Some companies in the private sector sometimes don't want to spend a lot of money on security," he adds. "Make your security posture part of your mission. Once a quarter...we want you to bring in the following people: your CEO, general counsel, CIO, CISO, chief data officer, head of procurement, head of HR, and your head of physical security. Have a discussion about enterprisewide security...because they all need to be part of your enterprise security posture."

Evanina also suggests conducting tabletop exercises that walk stakeholders through handling a data breach or hiring an individual who turns out to be sharing trade secret information.

"Walk through that crisis plan and identify who you're going to call, how you'll notify your stockholders and shareholders and share what you've done," Evanina adds.

The NCSC's work is just one part of the executive branch's action to mitigate China's activities. The U.S. Department of Justice also stood up a China Initiative, overseen by John Demers—assistant attorney general for the National Security Division—to protect U.S. technology.

"In addition to identifying and prosecuting those engaged in trade secret theft, hacking, and economic espionage, the initiative will increase efforts to protect our critical infrastructure against external threats, including foreign direct investment, supply chain threats, and

the foreign agents seeking to influence the American public and policymakers without proper registration," according to a fact sheet.

Since its inception in 2018, the China Initiative has led to numerous indictments for charges of trade secret theft and disclosure failures—like those brought against Tan and Lieber. It has also worked with companies that have had intellectual property or trade secrets stolen to prevent the thieves from turning that information into a profit.

For instance, Chinese company Fujian Jinhua allegedly stole intellectual property from U.S.-based chip manufacturer Micron. Micron coordinated with the initiative and was able to work with the U.S. federal government to file a civil lawsuit to prohibit Fujian Jinhua's ability to obtain the necessary materials to produce Micron's chips.

The U.S. Treasury Department's Committee on Foreign Investment in the United States (CFIUS) is also playing a role. The committee is required to review certain transactions that involve foreign investment in the United States—along with some real estate transactions by foreigners—to determine if they will impact America's national security.

In 2018, U.S. President Donald Trump signed into law the Foreign Investment Risk Review Modernization Act (FIRRMA). The law was designed to modernize CFIUS' role after congressional analysis by the U.S. Senate Intelligence Committee found that China was investing heavily in American technology firms to gain access to assets that could have national security ramifications.

FIRRMA allows the committee to review investment in U.S. businesses that own, operate, manufacture, supply, or serve critical infrastructure or create critical technologies. If the investment would allow a foreign

government to become a partial owner, the investment could be denied on national security grounds.

"FIRRMA has been relatively successful for a number of reasons—Chinese investment has declined about three-quarters," Lewis tells Security Management. "Some of that was the Chinese putting restrictions on wealthy Chinese moving money out of the country, but some of it was the response to the fact that efforts to buy high-tech companies are routinely denied now."

The United States and China did sign a historic trade agreement in January 2020, which included provisions on respecting intellectual property rights and enforcement against misappropriation of trade secrets and confidential business information. But many, including Lewis, are skeptical.

"IP protection has been part of the trade deal with China, but everyone I talk to doesn't believe it will have any effect," he says. "The Chinese will agree and then continue to cheat. So, we need to think of something beyond bilateral trade deals, and the chance for partnership is out there."

Instead, Lewis says the United States will need to partner with others to prevent Chinese investment or involvement until it changes how it acquires intellectual property and shields its domestic firms from competition. In conversations with representatives from the European Union and other regions, Lewis says they also said they need to tighten their controls on Chinese investment.

"The Japanese feel that way. The Australians feel that way. The Europeans are moving in that direction, so China's behavior is causing concern for everyone," Lewis says. "That's an opportunity for the [Trump] administration. They haven't been able to take advantage of it yet, but this isn't just the United States."

Ultimately, China must be required to honor its international obligations as a member of the World Trade Organization (WTO), he adds.

"Countries that are members of WTO need to hold China accountable for its lax enforcement of IP rules," Lewis says. "I don't see that happening, but that's what it would take—for people to say this kind of behavior is unacceptable."

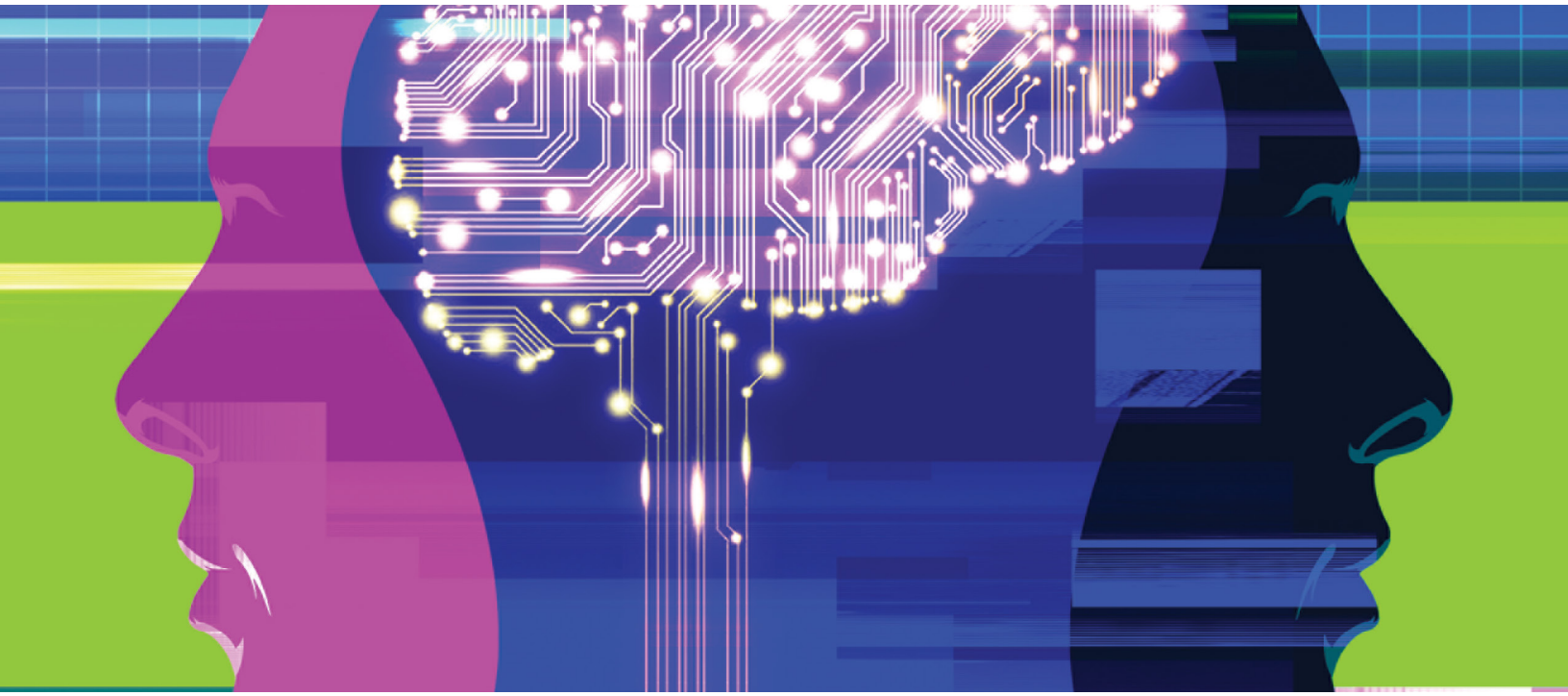
MEGAN GATES IS SENIOR EDITOR AT SECURITY MANAGEMENT. CONNECT WITH HER AT MEGAN.GATES@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @MGNGATES.

SECURITY MANAGEMENT

The Attacker Mentality

Through focus, patience, and nonlinear thinking, malicious actors create new paths into organizations. Defenders need to use attackers' own tactics against them.

By Val LeTellier



Society would be far less enjoyable if we all adopted an attacker mentality. Everyone's first thought upon meeting someone new would be how to manipulate them for personal gain. Each encounter would be based upon the assumption that there are no rules of engagement, political correctness, manners, morality, or conscience at play.

Attackers are comfortable doing things that most people aren't. They look for exploitable motivations and vulnerabilities to create self-serving situations. They are comfortable masquerading as someone else, building false relationships, and hiding the truth. For instance,

attackers have no qualms about following your CFO home to collect personal information, booking a room on your CEO's hotel floor and "getting to know" him or her at the hotel bar to collect details about the company, sending your IT staff cool gifts laced with malware, or even using Facebook to send your kids a malicious link hidden within a game.

These guys are different. They take it up notch or five. But what, exactly, sets them apart?

Singular mission focus. Professional attackers are not distracted by what is happening on the sidelines; they focus exclusively on mission achievement. They are not constrained by administration, bureaucracy, or budget, and they do not make decisions by committee. They know what they want, and they go for it.

If you ever wanted to know the comprehensive list of valuables you have access to, just ask an attacker. They will know because they are always sizing up people and opportunities for personal gain.

You may be surprised by what attackers consider valuable and why. It may sometimes be as obvious as money or intellectual property, or it could also be other items. In today's world, opportunities for financial gain are much broader than before. Attackers may seek different items, depending on whether they are thieves, conspirators, leakers, discontents, or opportunists. One's reputation, relations, personnel, speed of business, and mental wellness can be targets for specific attackers with specific agendas.

Using data as an example, the cybersecurity "CIA Triad" of confidentiality, integrity, and availability tells you that theft is not the only threat—an attacker could also harm your organization by clandestinely disrupting your data integrity or denying you or your customers access to your data.

Patience. Ever found yourself in the right place at the right time? Whether we attribute it to luck or serendipity, most of us also seek to create those situations for ourselves in our daily personal and professional lives, but our results are usually hit or miss. We simply can't be in all the right places just waiting for the right time to come around. But that is exactly what an attacker does.

In the cybersecurity world, digital "honey pot" websites allow attackers to lie in wait for unsuspecting victims to come to them. In the physical world, attackers tailgate by loitering near a door to a facility and following someone with legitimate access into the building.

Defenders face the immense challenge of shutting down paths they can't conceive of in the first place.

Their greatest advantage is your greatest challenge: the attacker only needs to be right once, but defenders must be right all the time.

Nonlinear thinking. While most people see a direct line between points A and B, attackers often look at how points D and F can get them to point B. They see patterns and then figure out when those patterns stop applying. They find the edge between "yes" and "no" and test how sharp that edge really is. They ask open-ended questions, begin with more than one premise, make deductions, and then infer ways forward. If that path is blocked, they repeat the process from the beginning. Attackers seeking weaknesses in software exploits often follow this process; the program is viewed holistically, leading to specific premises, deductions, and inferences that point to security gaps.

This linear thinking is applied within each phase of their attack: performing reconnaissance, scanning and enumerating, gaining access, escalating privilege, creating redundant access, and covering their tracks.

Attackers look at problems without blinders. They see the complete picture and never rule out an implausible option if it could help them achieve their goal. Defenders face the immense challenge of shutting down paths they can't conceive of in the first place.

Using social engineering, attackers exploit human nature.

Backward reasoning. Attackers visualize their goal and work backward, which allows them to identify all possible accesses and paths, especially ones unidentified and unprotected by defenders.

Known by various terms (backward chaining, reverse engineering, purposeful task analysis, retrograde analysis, or backward induction), backward reasoning is a well-recognized methodology. Before Amazon designers and developers start a new project, they write a hypothetical press release from the future, celebrating the success of a product. From there, they determine what needs to be done to get to that point of success. And it is the second of Stephen Covey's Seven Habits of Highly Effective People, "Begin with the end in mind."

In 2006, retail giant TJX Companies Inc. (TJX), experienced two notable examples of attackers working backward from the company's lucrative customer record data. Attackers used in-store job application computer kiosks to deploy malware through mouse/printer USB ports,

turning the devices into remote terminals with access to the main network. The firewalls on TJX's main network weren't set to defend against malicious traffic coming from the kiosks. Months later, attackers accessed an improperly secured Wi-Fi network from the parking lot of a Marshall's store in St. Paul, Minnesota, and exploited the deficiencies of the aging Wired Equivalent Privacy (WEP) wireless security protocol. More than 45 million records of customer payment data and untold revenue were lost.

By any means necessary. Although attackers maintain a single-mindedness in their focus, this does not mean they limit themselves to a single vector or approach. They use whatever works, whether it is within the virtual, human, or physical domains. What the average defender defines as "all possible attack vectors" is almost laughable to someone who has no rules.

THE ATTACKER MENTALITY AT WORK

The attacker mindset and approach were showcased in an attack against a major oil company in 2014. Unable to breach the company's computer network, attackers instead injected malware into the online menu of a Chinese restaurant popular with employees. When workers browsed the menu, some were socially engineered into unknowingly downloading code that provided the attackers a narrow foothold in the company's network. From there, the attackers found an opening to create a company identification badge that allowed them to pose as an IT vendor and get physical access to the firm's servers.

This operation demonstrated attackers' ability to exploit vulnerabilities across their operating environment, specifically within the digital, physical, and human

domains. Understanding the interconnectivity and interdependency of these domains and the aggregated risk they pose is a critical first step in the development of an organization's risk mitigation strategy.

The virtual attack surface. The escalating amount of attention that the virtual domain receives is merited. Risk within the digital domain is already extremely broad and exponentially growing, ranging from a lack of operational security to bad policies to bad code to executives' insecure home networks.

In the rush to launch competitive products and the prioritization of user convenience over security, manufacturers have often neglected necessary security safeguards. And thanks to our reliance on the Internet, attackers can now compromise almost anything—surveillance cameras, access control systems, microphones and cameras on smartphones and laptops, thermostats, vehicles, and industrial control systems.

The danger of combining an attacker mindset and widespread connectivity was exemplified in an attack against a North American casino in 2017. Using an Internet-enabled fish tank, attackers exploited sensors connected to a facility PC that regulated the tank's temperature, food, and cleanliness. As a result, 10 GB of private data was sent out to a device in Finland.

The security industry is most focused on the virtual attack surface, often developing automated digital countermeasures to identify a "silver bullet" solution. This approach addresses only part of the risk equation, and the effectiveness of each solution is reliant upon the diligence of those operating or engaging with the system. In the end, human behavior can either reinforce or degrade security measures.

The human attack surface. Em-ployees, trusted vendors,

and partners represent potential weak links. Using social engineering, attackers exploit human nature to access facilities, networks, and valued items. They can create well-researched and believable ploys to get what they need, incorporating techniques like pretexting, baiting, and quid pro quo.

Social engineering is a serious discipline with serious consequences. At DefCon's annual Social Engineering Capture the Flag event, the security practices and countermeasures of many top firms have been compromised by a talented attacker armed with just a phone.

A great example of social engineering is a 2007 attack on Antwerp's ABN Amro Bank. No one knows his real name, but the staff knew him as Carlos Hector Flomenbaum. He billed himself as a successful businessman, and he had frequented the bank for at least a year. The bank's employees loved Flomenbaum. He brought them chocolates, talked to them about non-diamond-related matters, and ultimately won their trust to the extent that he was given VIP access to the vault. One night in March 2007, he let himself in, broke into safety deposit boxes, and walked out the front door with $28 million in diamonds. The bank had a $2 million security system. Flomenbaum has yet to be caught.

The physical attack surface. If an attacker can gain access to the premises, he or she can quickly access sensitive information—both through the network and in hard copy. Inadequate physical security controls can render most technical controls useless. Interestingly, while firms traditionally expended most of their resources for physical security, it is now far subordinate to digital defense. And this change would be more dramatic if it weren't for the increasing attention paid to workplace violence.

To penetrate physical defenses, attackers collect data

via open sources and create sophisticated approaches that manipulate access control though social engineering, badge cloning, and close network access.

A well-used attack plan is the select placement of USB sticks labeled "payroll," "sensitive," or "personal" with embedded malware ostensibly dropped in public areas around a company. Well-meaning or curious employees will launch the attack themselves by connecting the USB to a work computer.

Across all attack surfaces, the attacker mentality is characterized by function over form, exploitation of simple vulnerabilities, being noisy or quiet depending on operational need, aggregating bits of seemingly meaningless data, utilizing unwitting or complicit surrogates, employing patience and gradual privilege escalation, creating backup access channels, and utilizing burnable channels to erase one's tracks.

USING THE ATTACKER MENTALITY FOR GOOD

The proper application of the attacker mentality can prevent an insider attack; protect the organization's most valuable resources, up-time, reputation, and jobs; and save security professionals from embarrassment and loss of stature.

But more specifically, the attacker mentality allows you to have insights normally unavailable in a risk assessment. It reveals a more comprehensive list of valuables, not just what matters to you, but also what others may covet; it identifies an attacker's most lucrative vectors; and it reveals attack vectors that can exist in places you've never imagined, such as partners, vendors, suppliers, insurance providers, HVAC equipment, printers, thermostats, videoconferencing software, vending machines, and fish tanks.

The bottom line is this: analyzing your organization using an attacker mentality allows you to identify the security gaps most likely to be used against you. Identifying those gaps and quantifying the associated risks are critical to obtaining stakeholder support and funding for insider threat programs and exercises.

Consider that famous Mike Tyson quote, "Everyone has a plan until they get punched in the mouth." An insider attack is like a punch in the mouth. Your conventional wisdom—your plan—takes a hit, and the world stops spinning for a second. You wonder where you are, what weakness the attacker exploited, what gaps you need to close, and which of your strengths you can rely upon to survive.

By leveraging the attacker mentality, you can have the all the knowledge that comes from a punch in the mouth, but without the broken jaw. To apply the attacker mentality to an insider threat program, first acknowledge that the status quo won't work. You have to accept that if you don't make some changes, the organization will be facing significant harm.

Second, change your own mentality. You cannot create effective insider defenses, risk management strategies, tabletop simulations, and security strategies if you are unsure how vicious, visionary, and committed your insider attackers are.

For many folks, the simple truth is that they are working against an enemy who is operating with a level of sophistication and determination they don't understand. Change your vocabulary, perspective, and approach. Stop sugar-coating attacks by using terms like "insider," "hacker," or "breach." Instead, use the terms "perpetrators" and "attack." There is a world of difference between saying you were "robbed" and "attacked," and the same difference exists between being "hacked" and "attacked."

Train yourself and anyone with network access to acknowledge that the world has changed. The new reality is that everyone must practice the same common sense security at work as they do in public places: beware of strangers approaching with unusual requests, seeking quick and unconventional actions, and applying pressure tactics. If even for just a second, question whether

Practice symmetrical thinking. Think like your attacker; holistically examine and map out your strengths and weaknesses.

the request, embedded link, or attachment makes sense. And if your gut check reflects any concern, pay attention.

Create environments that foster reality. Don't say "if it happens to us," "what are the chances," or "that is too far-fetched." Realize that there are two types of organizations—those that know they have been attacked and those that don't.

Practice symmetrical thinking. Think like your attacker; holistically examine and map out your strengths and weaknesses. Employ patience, nonlinear processes, and any means necessary in your reconnaissance and attack modeling. And start with the conviction that your security systems have exploitable gaps, that some of the people you trust with privileged access will fail to do the right thing at the right moment, that you have items of value that you're not protecting. For many businesspeople, this is just not possible. Many are incapable of stepping into an attacker's frame of mind; therefore, it makes sense to hire attack experts or "red teamers" to provide that perspective.

Red teaming is the practice of viewing problems from an adversary or competitor's perspective, a simulated attack

that prepares you for the real thing. The goal of most red teams is to enhance decision making by challenging assumptions, identifying the adversary's preferences and strategies, and acting as a devil's advocate.

Just as an attacker will use cyber, physical, and social engineering to find the most effective way to breach your defenses, so will red teams. If your red teams have firsthand experience attacking hardened facilities and workforces, the results of a red teaming exercise and a standard risk assessment will be even more pronounced.

Red teaming is focused on stopping the cut, not stopping the bleeding. It can help assess your countermeasures, prepare you for a real attack, and test your incident response measures before an incident occurs. It is the most effective test of your insider resiliency.

Therefore, the best time for a red teaming exercise is before your organization "goes live" to the public or its members, and the worst time is after an attack. If your organization or new product is already "live," the second-best time to red team is after a security review and/or enhancement. This allows you to test for any new vulnerabilities inadvertently created during the upgrade.

Red team testing can address both the inside and outside attacker perspectives, benign or malicious insiders, and actors that are being manipulated, guided, and protected by organized crime groups or intelligence services.

This testing will show you how attackers collect and analyze target data from personal observation, online research, and technical, physical, and human social engineering. It will demonstrate the privileged internal information and access that a determined attacker can realize in a short time with only moderate effort.

Effective red teaming will identify the security vulnerabilities that attackers would likely exploit first in an

attack. There should be no off-limits areas for the red team, because real attackers will use any means necessary to breach your technology, people, and facilities to access your critical resources. Your technology includes networks, applications, routers, switches, appliances, and devices. Your people include your staff, independent contractors, business partners, and anyone with trusted access. Your physical infrastructure includes your offices, warehouses, substations, data centers, and buildings.

Operating from the viewpoint of your adversary, members of a red team will collect public data on your organization and key officials. Using that information, they will evaluate potential vectors for attack and determine the best attack plan. They will launch a blended attack involving several facets of social engineering, physical penetration testing, application penetration testing, and network penetration testing. Then they will capture and report details on your response to the attacks and recommend mitigation solutions to close your security gaps.

The key to maximizing the effectiveness of your red-teaming effort is selecting a team with a strong attacker mentality, cutting-edge technical penetration and social engineering skills, and a strong track record of working against hardened facilities, networks, and workforces. Then give them as much freedom of access, time, scope, and methodology as you can.

Insider risk represents an existential threat to your organization's survival. Using privileged access and situational awareness, a single insider can cause immense financial loss, reputational harm, and even layoffs and bankruptcy. Your organization's future depends upon stopping their attacks.

To stop insiders, you need to know what an attacker would want from your firm, who has access to those

resources, and how an attacker would steal, alter, or deny access to them. Red teaming shows how real attackers will act, not merely how defenders imagine they will act.

That said, red teaming is not for the faint of heart. It often identifies weaknesses that you never knew you had and exploitable vulnerabilities that must be immediately closed. It provides a robust test of your incident response measures. It often is an eye-opening and sometimes embarrassing exercise for corporate security teams. But in the end, it is the preferred methodology for firms determined to do everything possible to secure themselves from insider attacks.

VAL LETELLIER HAS THREE DECADES OF RISK MANAGEMENT EXPERIENCE IN THE PUBLIC AND PRIVATE SECTOR. HE IS THE CHAIR OF INSIDER THREAT WORKING GROUP OF THE ASIS DEFENSE & INTELLIGENCE COUNCIL AND A MEMBER OF THE INSA INSIDER THREAT SUBCOMMITTEE.

SECURITY MANAGEMENT

Breach of 150,000 Surveillance Cameras Sparks Credential Concerns

Is your security secure? With more and more security devices being connected to networks, they are also exposed to network-based attacks and hacks.

By Claire Meyer

In the latest iteration, up to 150,000 security cameras installed in schools, hospitals, factories, and businesses were compromised, giving outsiders access to video from Tesla factories, prisons, psychiatric hospitals, and more.

Hackers claim to have breached surveillance company Verkada, which issued a statement that is it investigating the scale and scope of the incident, and that it has notified law enforcement. Allegedly, the attack was unsophisticated, using a privileged administrator account to gain access to the system, the BBC reported. A Verkada spokesperson responded that all internal administrator accounts have been disabled during the investigation to prevent further unauthorized access.

According to Bloomberg, which broke the news of the

breach yesterday, some of the cameras used facial recognition technology and analytics to identify and categorize people in video footage. The hackers also claimed to have had access to the full video archive of all Verkada customers—including live feeds, archived video, and audio.

One of the alleged hackers, Tillie Kottmann, told Bloomberg that the international hacker collective had intended to show the pervasiveness of video surveillance and ease with which it could be compromised—especially when devices are connected as part of the Internet of Things (IoT). Kottmann said that the collective gained access to the system on Monday morning, and has since lost access to the system.

"With IoT systems we now have a new dimension to cybersecurity," says Coleman Wolf, CPP, CISSP, senior security consultant for Environmental Systems Design, Inc., and a member of the ASIS International IT Security Community. "Whereas we used to be concerned with confidentiality integrity and availability of data, now we have the added concern of safety. The systems now have the ability to monitor and control physical world actions, and people need to understand the potential risks of this."

In addition, he says, "people need to perceive IoT devices as computers that can be hacked when put online rather than as mere appliances."

But security professionals remain behind the curve when it comes to cybersecurity. According to the Genetec State of Physical Security 2020 report, released in December 2020, only 31 percent of security professionals were focusing on cybersecurity or cyber hardening projects, and 29 percent were evaluating cybersecurity tools to improve physical security environments.

"With cyber concerns as a result of the pandemic on

the rise, and most physical security deployments remain on-premises, it is important that the physical security industry prioritize cyber hardening practices to get ahead of this major risk," the report said.

Genetec CSO and VP of Cloud Solutions Christian Morin commented on the Verkada breach, explaining that "as an industry, and as manufacturers in physical security, we cannot take these hacks lightly. The potential broad-reaching impact of these hacks on physical security systems, including providing a beachhead to

"...it's imperative for physical security professionals to partner with IT/InfoSec experts."

facilitate lateral movement onto networks, resulting in data and privacy breaches or access to critical assets and infrastructure, cannot be understated. It is our responsibility and duty to users of our technology to prioritize data privacy and cybersecurity in the development, distribution, and deployment of video surveillance systems."

He adds, "Given the nature of the technology used to implement physical security systems today, and the fact that these systems are more connected now than ever to achieve various business goals, it's imperative for physical security professionals to partner with IT/InfoSec experts."

These partnerships enable security professionals to better evaluate physical security systems' cyber risk and assess manufacturers' and integrators' ability and willingness to follow best practices.

Elisa Costante, vice president of research at IoT risk mitigation company Forescout, said that connected cameras are meant to provide an additional layer of security to the organizations that install them.

"Yet, as the shocking Verkada security camera breach has shown, the exact opposite is often true," she said in commentary shared with Security Management. "Worryingly, the attack wasn't even very sophisticated and didn't involve exploiting a known or unknown vulnerability. The bad actors simply used valid credentials to access the data stored on a cloud server.

"In this case, the bad actors have seemingly only resorted to viewing the footage these cameras have captured," she added. "But they are likely able to cause a lot more damage if they choose to do so, as our own research team has discovered. We were able to intercept, record, and replace real-time footage from smart cameras by exploiting unencrypted video streaming protocols and performing a man-in-the-middle attack. This effectively gives criminals a virtual invisibility cloak to physically access premises and wreak havoc in the real world."

Costante recommended organizations ensure that they have a comprehensive device visibility and control platform in place, which could help them adequately assess their risk and monitor for vulnerable devices or unauthorized access.

But managing credentials, especially when third parties are involved, can be challenging. Daniel dos Santos, research manager at Forescout, tells Security Management that "the credential management part is very difficult. If there are known, hard-coded, default, or weak credentials on the device, they can be detected if they traverse the network in cleartext or by testing the devices directly."

An IoT posture assessment engine example from Forescout can be reviewed here.

"If found to be vulnerable, then the organization can act to assess and mitigate risk by changing those creden-

tials," he says. "Alternatively, if the credentials are shared for access with a system provider, the organization can, and should, monitor and even enforce that their devices have incoming/outgoing connections only to trusted IP addresses or domains associated to that provider."

To monitor for credential leaks or breaches, Morin recommends looking for various indicators of compromise (IOCs) within the security operations center.

"For example, if leaked credentials are used to login to one of your system chances are, they will be used by

Compromised credentials are one of the most prevalent ways threat actors gain access organizations' networks.

someone that is located in another country which would trigger an impossible travel event," he tells Security Management. "There are also services/firms that specialize in providing information as it pertains to breaches that could impact an organization by scouring the dark web, often referred to as post-breach detection. This would alert an organization that sensitive information/credentials are available in the wild and ready to be exploited."

Compromised credentials are one of the most prevalent ways threat actors gain access organizations' networks. These credentials are often obtained via phishing attempts sent to targets' email inboxes, Morin adds.

"Fortunately, this is also one of the easiest types of attacks to protect against and in some cases eliminate altogether," he says. "However, many organizations continue to fail to implement some of the simple controls that can really help.

"In the end, it is important to remember that there is

no silver bullet or single control that solves everything," he continues. "Multiple controls are actually needed to improve your posture, and this is often referred to as defense in depth."

Some key controls that Morin says could help organizations fight credential compromise are:

Implement multifactor authentication on accounts. This prevents threat actors from login in using solely the username and password combo that could be harvested through phishing or previous breaches.

Segregation of duty by ensuring that privileged accounts are few, tightly controlled, and only used for their intended purposes.

Employ the principle of least privilege, which allows to limit the scope of the damages in the event of a breach.

Monitor IOCs, such as such as impossible travel (logging in from two locations on opposite sides of the world at once, for example). This would allow to detect these breaches much more rapidly.

Organizations can also mitigate risk by conducting thorough vendor risk assessments before buying in.

"As part of this assessment it's important for organizations to ask the right questions of their vendors and make a risk decision based on the nature of the information that this vendor will be processing/handling," Morin says. "In the case of video surveillance or access control systems, the impact could be very high for many organizations. It's important to ensure that any vendor meets or exceeds your own organization's security controls and make the call on whether the risk is acceptable or not when they do not."

Security professionals can ask:

- Does the vendor employ multifactor authentication (MFA)?
- Does the vendor perform regular penetration tests?
- Was the vendor victim of any breach?
- Does the vendor have a secure software development process?

In addition to asking questions, security leaders should ask for proof to support the vendor's answers. Asking for a third-party certification—such as ISO27001, Morin says—will further assure that cybersecurity controls are properly implemented.

Last but not least, organizations should request audit rights, "so that you can see for yourself at any point that your data is handled appropriately," he adds.

"What is very important to understand is that cybersecurity is a shared responsibility," Morin says. "All parties involved in the system development, implementation, and operation have a critical role to play. It is important that manufacturers, integrators, and end users embrace this fact and work together to address this risk." ◪

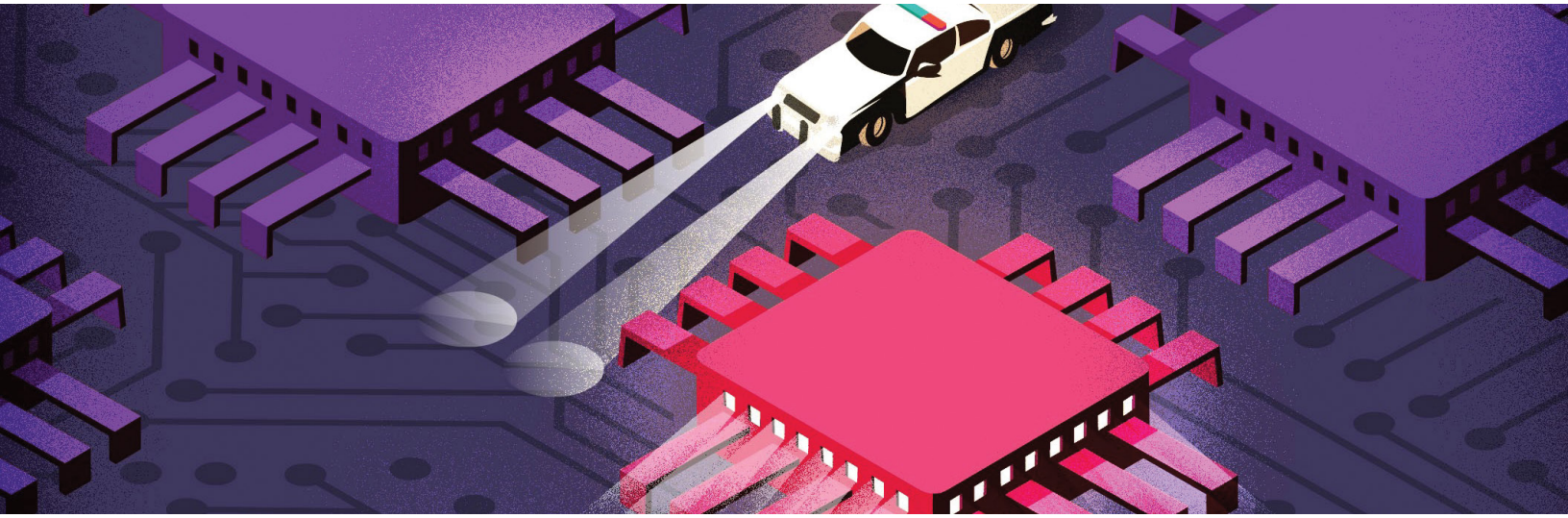
CLAIRE MEYER IS MANAGING EDITOR FOR SECURITY MANAGEMENT. CONNECT WITH HER ON LINKEDIN OR VIA EMAIL AT CLAIRE.MEYER@ASISONLINE.ORG.

SECURITY MANAGEMENT

A Patrol Problem

Organizations are getting better at patch management, but they still fail to invest in capabilities to detect and respond—quickly—to data breaches, an annual report finds.

By Megan Gates



The FBI Citizens Academy is a staple of the Bureau's community building initiative. Held over the course of six to eight weeks in cities throughout the United States, FBI agents educate business, religious, civic, and community leaders about how the Bureau investigates crimes and protects public safety.

When John Loveland, global head of cybersecurity strategy and marketing for Verizon, attended the academy, the agent in charge discussed tactics the FBI uses to detect bombers and provide security at large scale events—such as the Boston Marathon. One common approach is placing police cars and officers near major intersections to

monitor traffic and identify suspicious activity.

"There was a question in the course of, 'Are you relying on those metro police officers to detect if there's a truck bomb?'" Loveland says. "The agent's comment was, 'If I have to rely on those guys, I've screwed up.'"

The FBI instead relies on investigative and detection methods that would ideally alert the Bureau to a potential bomber long before he or she went by one of those police officers stationed at a traffic ramp. But this is often not the approach that organizations are taking towards cybersecurity.

"We're spending a lot of time putting cop cars at the entrances to our networks to keep bad guys out, but at the end of the day, the exploits are such that some hackers are going to get through," Loveland says. "Companies have to be spending as much if not more on tech and solutions that help quickly detect when there's an anomaly in the system."

Loveland's assessment is based on findings from the 2020 Verizon Data Breach Incident Report (DBIR), which found that while containment time for a data breach is down to days or less "discovery in months or more still accounts for over a quarter of breaches."

Now in its 13th year, the report has grown to analyze 32,002 security incidents of 157,525 total incidents from data submitted by 81 contributors from 81 countries. Verizon defines incidents as "security events that compromise the integrity, confidentiality, or availability of an information asset."

The report also includes analysis by industry—broken out into 16 verticals—to help practitioners improve their ability to defend against and mitigate the effects of data breaches (an incident that results in confirmed disclosure of data to an unauthorized party), of which there were a confirmed 3,950 in 2019.

There were a few key themes presented in the data this year. The first was that the use of ransomware continues to grow—representing 20 percent of all malware-related breaches in 2019. Verticals that saw the greater rise in ransomware attacks were against education and state and local governments.

"We saw a trend in that direction that just really caught fire," Loveland adds. "I venture to say that a majority of the tier 1, tier 2 municipalities have faced some form of ransomware attack."

Ransomware is primarily being introduced to the environment through phishing, which is used to capture user credentials to gain access to Web applications, Loveland says.

This has even greater consequences as the world continues to move towards the cloud and rely on security as a service (SaaS) applications.

We're spending a lot of time putting cop cars at the entrances to our networks to keep bad guys out.

"You're expecting [Amazon Web Services] and these platforms to have high level, high grade security to prevent break-ins," Loveland explains. "But a point of vulnerability remains with compromised user credentials. Robust security is possible, but if someone gets ahold of your or my credentials and uses it to access the system—all those defenses are for naught."

And the individuals often behind these breaches are external actors (70 percent) typically associated with organized criminal groups (55 percent of breaches). Most of these breaches were carried out for financial gain (86 percent) and were discovered in days or less (81 percent).

"One thing that gets press attention is nation-state actors looking for intellectual property—that's stolen or used for competitive advantage," Loveland says. "That occurs in manufacturing and the public sector, but by and large these breaches are financial in nature."

Loveland also explains that breaches are perpetrated by insiders, but that does not always mean the insider is acting maliciously. Many of these breaches are the result of errors or misconfigurations in systems that inadvertently cause a data breach.

"...in spite of what you may have heard through the grapevine, external attackers are considerably more common in our data than are internal attackers, and always have been," according to the report. "This is actually an intuitive finding, as regardless of how many people there may be in a given organization, there are always more people outside it. Nevertheless, it is a widely held opinion that insiders are the biggest threat to an organization's security, but one that we believe to be erroneous. Admittedly, there is a distinct rise in internal actors in the data set these past few years, but that is more likely to be an artifact of increased reporting of internal errors rather than evidence of actual malice from internal actors."

The report's authors saw this most frequently in the healthcare vertical, where internal actors were responsible for approximately 50 percent of breaches. This is because they are working in a "fast-paced environment where a huge amount of work must be done and is also facilitated by paper," Loveland says. "They often don't have controls that are up to snuff—leaving lots of room for errors."

Errors have always been common in industries with mandatory reporting requirements—like public administration and healthcare—but are now rising in other industries, too.

"The fact that we now see error becoming more apparent in other industries could mean we are getting better at admitting our mistakes rather than trying to simply sweep them under the rug," according to the report. "Of course, it could also mean that since so many of them are caught by security researchers and third parties, the victims have no choice but to utter 'mea culpa.'"

In fact, security researchers were the individuals most likely to alert organizations of a data breach—notifying

Organizations should be looking to enhance their detection and response capabilities by creating more points to monitor movement through their network and on devices.

organizations roughly 50 percent of the time, six times higher than in 2018. Less than 10 percent of breaches were reported by internal employees.

This demonstrates the gap that continues to exist in organizations' ability to detect when they have experienced a breach and that the focus on perimeter protection—instead of detection and response—is misguided.

For instance, organizations should be looking to enhance their detection and response capabilities by creating more points to monitor movement through their network and on devices. These measures are also imperative given the rise of remote work in response to the coronavirus pandemic.

"How are companies extending the security fabric outside their four walls?" Loveland asks. "How do you install that same behavior and vigilance at home that you have in the office?"

One positive finding from the data, Loveland adds,

is that there has been a steady decline in vulnerability exploits being used to compromise organizations. A common example of this tactic is the Equifax breach, where a Web application was compromised because the company failed to patch a known security flaw.

"We're seeing patching and patch management start to have an impact in reducing some of the vulnerability exploits and also reducing things like Trojans," Loveland says. "Hygiene is on the increase; it's helping reduce those traditional attacks."

MEGAN GATES IS SENIOR EDITOR AT SECURITY MANAGEMENT. CONNECT WITH HER AT MEGAN.GATES@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @MGNGATES.

SECURITY
MANAGEMENT

ASIS INTERNATIONAL
Advancing Security Worldwide®

Security Management is the award-winning publication of ASIS International, the preeminent international organization for security professionals. *Security Management* is written primarily for security professionals. It also makes vital security information understandable to a general business audience, helping ASIS International advance security worldwide. Readers receive timely information on emerging security threats and practical solutions, which they can use to protect people, property, and information.

To join ASIS International and become a subscriber to *Security Management*, visit asisonline.org/membership/join.