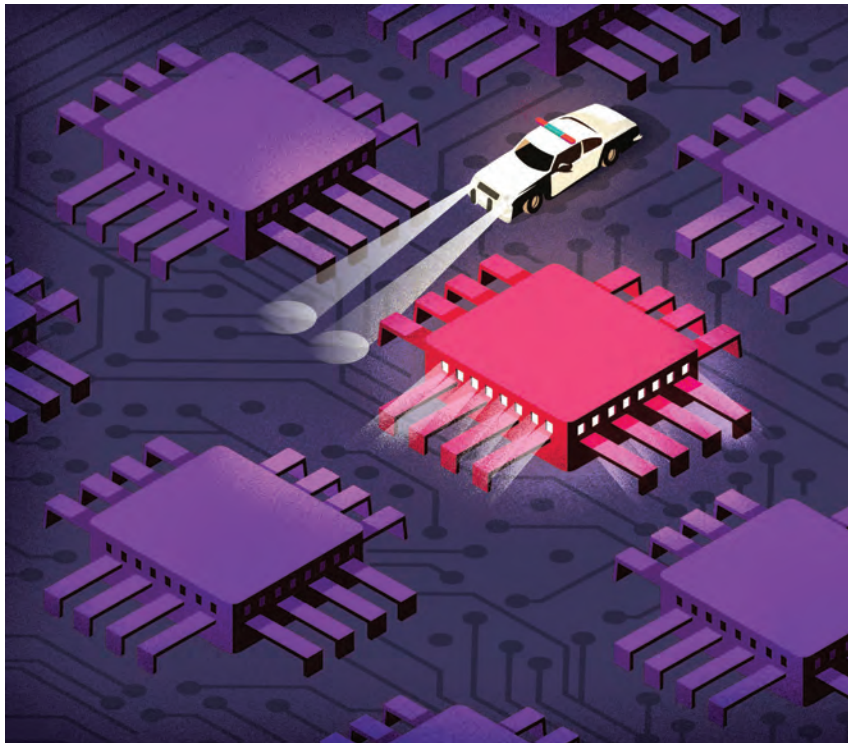


ILLUSTRATION BY RAUL ARIAS

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."

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

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.

"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.

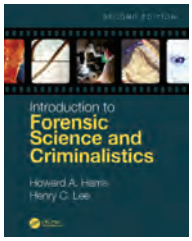
"The fact that we now see error becoming more apparent in other industries could mean we are getting better at admitting our mistakes rather than trying to simply sweep them under the rug," according to the report. "Of course, it could also mean that since so many of them are caught by security researchers 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 organi-

FORENSIC SCIENCE

BY HOWARD A. HARRIS AND HENRY C. LEE. CRC Press; crcpress.com; 420 pages; $89.95.

THE TOPIC of forensic science and criminalistics can be of interest to the security profession in the identification and protection of evidence in an investigation, but it is not a function that would normally be the responsibility of a security professional.



The second edition of *Introduction to Forensic Science and Criminalistics* is of value to students of or those engaged in the collection and analysis of evidence in a criminal case.

The authors of the book are leaders in their profession and offer many years of experience, sharing vast original content and knowledge within the publication. As a criminalistics publication it provides an advanced level of information that is current and valuable. The writing style is organized, concise, and easy to read. The chapters follow a logical sequence covering the topics within the book, including physical evidence, crime scene processing, questioned documents, digital evidence, biological evidence, explosives, and drugs, among other things.

Color photographs, charts, and lists within the publication provide excellent visual context to the book, supporting and enhancing the text. The book provides an abundance of references to back up its data and for future reading. The in-depth index allows for easy retrieval and review of relevant information.

Overall, this is an excellent book for its intended audience. It would be of value to those in the security profession who seek to expand their knowledge of this scientific discipline and to have the publication as a professional reference.

REVIEWER: *Daniel Benny, CPP, PCI, holds a PhD in Criminal Justice and is a tenured associate professor in intelligence and security studies at Embry-Riddle Aeronautical University Worldwide Campus. He is the author of seven textbooks on security matters and has been a member of ASIS International since 1976.*

WHERE IN THE WORLD DID THE MOST BREACHES OCCUR?

The 13th edition of the *Verizon Data Breach Incident Report,* published in 2020 on data collected from 2019, identified a total of 157,525 security incidents around the world—32,002 of which met Verizon's quality criteria for analysis.

North America led the field with 18,648; followed by Europe, Middle East, and Africa with 4,209; Asia and the Pacific with 4,055; and Latin America and the Caribbean with 87. The report said 5,003 incidents were reported, but they occurred in unknown locations.

One reason North America may have the highest number of incidents is because of its data reporting standards for industries, including healthcare and public administration.

"Therefore, the number of incidents and breaches are likely to be higher than in areas with less stringent disclosure requirements," according to the report. "Also, it must be admitted that while this report is becoming increasingly global in scope, many of our contributors are located in and are primarily concerned with North American organizations."

North American organizations saw a high number of financially motivated attacks against Web application infrastructure, leveraging stolen credentials obtained through social engineering attacks. Europe, the Middle East, and Africa were often targeted by attackers combining hacking techniques that leveraged stolen credentials or known vulnerabilities. The Asia and Pacific region saw a high number of financially motivated actors targeting their systems.

zations 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.

External attackers are considerably more common in our data than are internal attackers.

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.

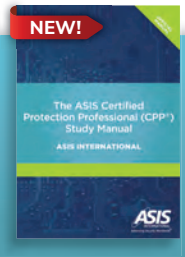
"We're seeing patching and patch management start to have an impact in reducing some of the vulnerability exploits and also reducing things like Trojans," Loveland says. "Hygiene is on the increase; it's helping reduce those traditional attacks."

@ To read the Verizon *DBIR,* visit SM Online.

ASIS INTERNATIONAL

Introducing the official
CPP STUDY MANUAL

The ASIS Certified Protection Professional (CPP®) Study Manual, our brand-new comprehensive study resource, explores the seven CPP domains, concepts, and terms, and helps you master the key content areas covered on the CPP exam.



Secure your copy today
asisonline.org/CPP-Manual