USE DATA TO CLOSE THE CUSTOMER SECURITY GAP

By George Hulme

AUGUST 2016 | US$25

Channel Partners™

TABLE OF CONTENTS

Channel Partners™

ABOUT THE AUTHOR

GEORGE V. HULME is an internationally recognized security and business technology writer. For more than 20 years Hulme has written about business, technology and IT security topics. From March 2000 through March 2005, as senior editor at InformationWeek magazine, he covered the IT security and homeland security beats. His work has appeared in CSOOnline, ComputerWorld, Network Computing, Government Computer News, Network World, San Francisco Examiner, TechWeb, VARBusiness and dozens of other technology publications.

linkedin.com/in/georgehulme
@georgevhulme

USE DATA TO CLOSE THE CUSTOMER SECURITY GAP

By George Hulme

SPANISH PHILOSOPHER GEORGE SANTAYANA SAID, "THOSE WHO CANNOT REMEMBER THE PAST ARE condemned to repeat it." Unfortunately, when it comes to cybersecurity, the same mistakes are being made by enterprises over and over, year after year. That is one of the most salient takeaways from the Verizon 2016 Data Breach Investigations Report (DBIR). Now in its ninth year, the DBIR analyzes roughly 2,260 confirmed data breaches and more than 100,000 reported security incidents. Verizon and 66 other technology and security firms contributed to the report.

While breach stats are bad news for enterprises, it does mean that there is much more work that needs to be done. Solution providers that can help enterprises better align their security products and policies — and better identify and respond to those that do get through — will be indispensable to customers. It's a big undertaking that's underway now, and will be for years to come: Research firm MarketsandMarkets expects the global cybersecurity market to grow from $106.32 billion in 2015 to $170.21 billion by 2020, compounding annually at nearly 10 percent. Given the long shelf life of malware — the DBIR shows 99.9 percent of exploited vulnerabilities hit more than one year after release of a patch — and the ingenuity of attackers mean security is the poster child of a future-proof practice.

Go Phish

The DBIR studied about 636,000 phishing emails:

89% – of attacks come from organized crime syndicates	**30%** – of messages were opened by the target, up from **24%** in 2015 and **11%** in 2014	**13%** – of people tested that clicked on a phishing attachment

Data: DBIR

SAME ATTACKS, DIFFERENT YEAR

Enterprises keep getting stung by the same attackers targeting the same vulnerabilities for the same reasons. According to the DBIR, 89 percent of all attacks are motivated by financial gain or espionage. Attackers mostly get in through a limited number of well-known means — in fact, 85 percent of successful exploits relied on the top 10 known vulnerabilities. And a startling 63 percent of data breaches involve using weak or stolen default or user credentials.

"You might say our findings boil down to one common theme: the human element," Bryan Sartin, executive director of global security services, Verizon Enterprise Solutions, said in a statement. "Despite advances in information security research and cyber detection solutions and tools, we continue to see many of the same errors we've known about for more than a decade now."

One of the biggest categories continues to be "miscellaneous" human errors, such as improper disposal of company information, IT system misconfigurations and lost or stolen hardware. Twenty-six percent of these assorted errors also involve users sending sensitive information to the wrong places.

"I still believe a lot of this is a people problem," says Chris Blow, senior security advisor at MSSP Rook Security. "Security awareness and having people in the right mindset, regardless of their role, are still extremely important. So much focus is on IT for this type of thing, but the focus should be companywide. I don't care if you're a server admin or a janitor: There is risk in every position of a company."

While few security experts would disagree with Blow, security awareness training, at only about $1 billion annually, is one of the smaller cybersecurity market segments; however it is growing at a hefty 13 percent annually.

DBIR ATTACK TRENDS

This year's report also found considerable use of a three-pronged attack. First, an individual is hit by a successful phishing attack that entices the user to click on a link within an email that is designed to drop a malicious payload on the user's system. From there, the attacker will sniff around for data and credentials to steal. Those credentials may be used to break into other systems on the network. Stopping such attacks would require traditional investments in tools like anti-spam and anti-malware software, but also — a much bigger undertaking that has a services angle — in identity management.

As we discuss in the sidebar on this page, if more customers worked with an adviser to craft a security framework and logically plan their cybersecurity investments, they'd be much more successful at managing common attacks, as was discussed at a recent identity conference.

"The planning process is so important, and companies still surprise me today in their lack of planning," said Lawrence Wolf, managing partner at strategic security and risk consulting services firm Edgile. "They'll buy the technology without planning what they're going to do with it, which typically leads to what I would call a 'one and done' technology implementation. The problem is, it's never really 'done.'"

Also worth noting is the importance of web application security, which proved its worth this year. In the DBIR, web application attacks were the most common exploit type, with the number of web application breaches up an eye-opening 33 percent year over year. In almost all of these attacks, 95 percent, attackers were motivated by financial gain.

9 Directions of Attack

Customers may fail to understand all ways they're being targeted. Each of these must be addressed in a comprehensive plan; you can find much more detail and recommendations in the full DBIR.

Web Application Attacks
Any incident in which a web application was the vector of attack. This includes exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms.

Insider and Privilege Misuse
Incidents involving unapproved or malicious use of organizational resources fall within this pattern. This is mainly insider-only misuse, but outsiders (due to collusion) and partners (because they are granted privileges) show up as well.

Miscellaneous Errors
Incidents where unintentional actions directly compromised a security attribute of an information asset. This does not include lost devices, which are grouped with theft instead.

Physical Theft and Loss
Pretty much what it sounds like — any incident where an information asset went missing, whether through misplacement or malice.

Crimeware
Any incident involving malware that did not fit into a more specific pattern. The majority of the incidents that comprise this pattern are opportunistic in nature and have a financial motivation behind them. This pattern frequently affects consumers and is where "typical" malware infections will land.

Point-of-Sale Intrusions
Remotely launched attacks against environments where card-present retail transactions are conducted. PoS terminals and PoS controllers are the targeted assets. Physical tampering or swapping out of devices are also common.

Payment Card Skimmers
Incidents in which a skimming device was physically implanted (tampering) on an asset that reads magnetic stripe data from a payment card. Think ATMs and gas pumps as well as PoS terminals.

Cyber Espionage
Incidents in this pattern include unauthorized network or system access linked to state-affiliated actors and/or exhibiting the motive of espionage.

Denial-of-Service Attacks
Any attack intended to compromise the availability of networks and systems. Includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service.

Source: DBIR

Customers are willing to spend to try to fix the problem — according to MarketandMarkets, the global application security market will grow from $1.24 billion this year to $6.77 billion by 2021. That's a rapid annual growth rate of nearly 25 percent.

HOW TO HELP

"There are many challenges when it comes to information security, as it's a moving target," says Ben Rothke, senior security consultant at Nettitude. "When you have dynamic environments, often without enough staff and budget, bad things will happen."

For customers in the current hiring environment, ensuring that they have an adequate and well-trained security staff is difficult. Intel Security recently released a Hacking the Skills Shortage report in which 82 percent of 775 IT decision-makers who are involved in cybersecurity said there's a workforce crisis. Most, 71 percent, said a lack of talent has had a negative effect on their organizations.

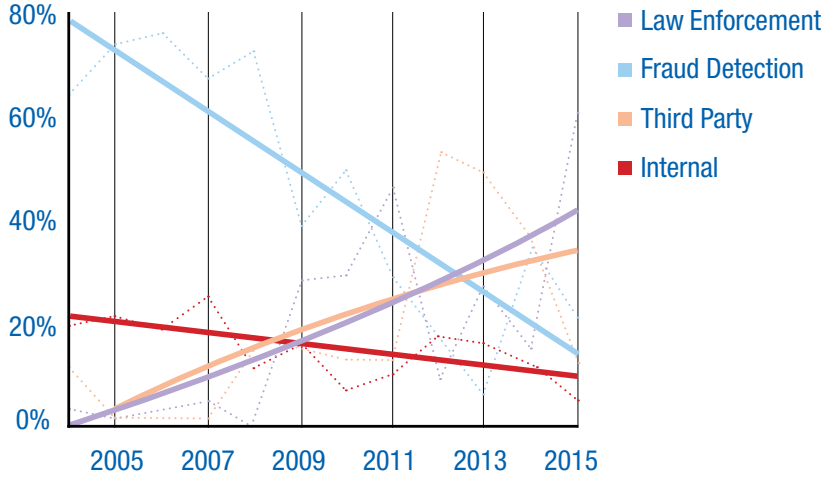
The good news for partners selling cybersecurity products and services is that almost nine out of 10 respondents said that advancements in cybersecurity could compensate for a skill shortage, with spending on better technology substituting for scarce human capital.

Still, tools will get them only so far.

Blow says that much of the reason attackers are able to infiltrate is because enterprises are deploying technology without providing the right personnel training and organizational processes to support a strong security posture.

Who's Spotting the Breaches?

Customers who think their own internal IT teams will detect breaches are largely mistaken. Most notifications come from law enforcement organizations that have taken down botnets. At that point, the data is compromised.



Source: 2016 Data Breach Investigations Report

"I see companies all the time that are still thinking that buying tech is going to fix the problem," he says. "They'll buy stuff and then it just sits in a default state. There's no tuning, and no professional services to get the thing up and running."

An understanding that making security technologies work effectively requires budgeting for training and services is a good start — but it's certainly not enough on its own. The 2016 DBIR report reiterated a need for enterprises to focus on the basics. Solution providers should sit down with customers and make sure that, at minimum, the following are in place:

- Awareness of attack patterns that are most common for the industry. For example, health care firms are currently hot targets for ransomware, while a bank with remote ATMs or a gas station owner may need to watch for sophisticated skimmers.
- A policy to use two-factor authentication for internal systems and select other applications, such as popular social networking sites.
- A plan to patch software and systems, including all end-user devices, servers, routers and switches, promptly.
- The ability to monitor all inputs, including reviewing all logs to help identify malicious activity.
- Encryption of data in transit and at rest. If the files on a stolen device are encrypted, for example, it's much more difficult for attackers to access. It also has implications for reporting.
- Staff training must happen continually. Developing security awareness within the customer organization is critical, especially with the rise in phishing attacks.
- Data classification will help prioritize what to protect, and how. Customers may then also better limit who has access to sensitive information.

Blow adds that solution providers are in a good, but largely untapped, position to help enterprises improve their processes.

"The findings consulting companies are delivering should have a dedicated section for people and process improvement," he says. "Help the client get down to the root cause. Is it because [IT asset] inventory isn't up to date? Is it because servers can't be rebooted due to availability issues and therefore patches aren't implemented properly? There are so many people/process-based questions that should be asked while on-site, but aren't."

Most all the experts interviewed agree that, for a sustainable fix for enterprises, helping them to better manage to objective standards, such as ISO/IEC 27001, PCI DSS or those from NIST, is an ideal starting point.

"Imagine a Fortune 1000-level firm, they would need an external consultant to come in and create policy and processes, and work with them to take information security much more seriously," says Rothke. "Everything from awareness, secure application design, physical security, logging, monitoring — it all needs to be brought into scope. It is a long-haul, and it's a matter of changing a mindset."