ATTENTI
h4x0r5
WA
FREE TO GOOD HOME:
Half a million personal information records
FLASH DoS TONIGHT!
No signup required. First to join picks the target!
WANTED
Acme Corp
For flagrant insecurity and social injustice
$10 ad

DBIR SNAPSHOT: INTELLECTUAL PROPERTY THEFT

A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting & Information Security Service, Police Central e-Crime Unit, and United States Secret Service.

DATA BREACH INVESTIGATIONS REPORT

A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police,
Dutch National High Tech Crime Unit, Irish Reporting & Information Security Service,
Police Central e-Crime Unit, and United States Secret Service.

Verizon's annual Data Breach Investigations Report (DBIR)[1] analyzes forensic evidence to uncover how sensitive data is stolen from organizations, who's stealing it, why they're doing it, how the victims responded, and what might have been done to prevent it. This Snapshot draws information from the DBIR data set, but gives highlights focused exclusively on 85 confirmed data breaches over the last two years resulting in the theft of intellectual property (IP)[2].

As with the annual DBIRs, the findings in this Snapshot are arranged using the Vocabulary for Event Recording and Incident Sharing (VERIS)[3] framework and based on breaches investigated by Verizon's RISK Team or one of our partner organizations, which include the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit, and United States Secret Service. Also like the DBIRs, all incidents in this snapshot involved confirmed unauthorized access and exfiltration of non-public information rather than potential exposures and other data-at-risk events.

DBIR SNAPSHOT: INTELLECTUAL PROPERTY THEFT

SUMMARY OF FINDINGS

During presentations and discussions on the DBIR, we're often asked about targeted attacks, state-sponsored campaigns, industrial espionage, insider abuse, and other genres of breaches tied closely to intellectual property (IP) theft. This is understandable, since the issue is close to the heart of several industries such as manufacturing, government, financial and technology services, etc. Many hold that these incidents differ in various ways from those involving payment cards, personal information, and other fraud-driven attacks, and our data set appears to support this position.

In almost all other areas we analyze, the target is nearly always one of opportunity. This is overwhelmingly the case with regard to verticals such as Retail or Accommodation and Food Services, but also mostly true of the Finance and Insurance industry and the Healthcare sector as well. However, when it comes to IP theft, the targeted nature of the attacks considerably changes how they are conceived and carried out. The fact that it is usually a different kind of threat agent—those looking for highly sensitive information to be used for a specific purpose, as opposed to those only looking for a quick cash out—also changes the game. In fact, their highly targeted nature makes these types of attacks more closely akin to each other than if we were to do an industry-specific slant.

When it comes to IP theft, the targeted nature of the attacks considerably changes how they are conceived and carried out.

[1] To learn more about the DBIR series, visit verizon.com/enterprise/dbir.

[2] For the purposes of this report, "Intellectual Property" includes the following data varieties in VERIS: trade secrets, classified data, and copyrighted/trademarked material.

[3] For more information on VERIS or any of the classifications used in this report, see veriscommunity.net.

VICTIM DEMOGRAPHICS

Since organizations of all types produce and use IP, one might assume that IP theft would stretch across industry lines. And one would be correct; our investigations encompassed a wide range of victims suffering such losses. The financial services and public administration verticals account for two-thirds of the breaches in this dataset, while information/technology services and manufacturing split the remainder. The majority of these organizations were based in North America, but Asian and European victims are represented as well. All in all, these findings support the notion that adversaries target IP as a shortcut to attaining some manner of strategic, financial, technological, or related advantage.

Adversaries target IP as a shortcut to attaining some manner of strategic, financial, technological, or related advantage.

Table 1. Organizational size (number of employees) by number of breaches involving Intellectual Property theft

1 to 10	2
11 to 100	10
101 to 1,000	11
1,001 to 10,000	31
10,001 to 100,000	33
Over 100,000	14

In a departure from industry-centric subsets of our caseload, victim size tilts noticeably toward the upper end of the scale. Since larger organizations tend to have more (and/or more well-known) IP, this reflects their status as a prime target. At the same time, they typically have more resources to commit to a stronger security posture, so stealing their prized possessions often requires a different strategy. The following sections highlight some of the important aspects of that strategy.

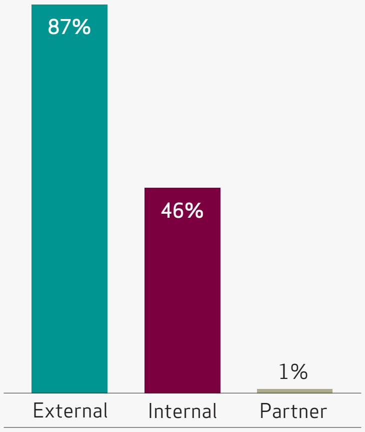
THREAT AGENTS

Entities that cause or contribute to an incident are referred to as threat agents. VERIS recognizes three main categories of agents: those originating outside the victim organization (external), those inside the victim organization (internal), and those involving any third party sharing a business relationship with the victim (partner).

However you slice it, the DBIR data set consistently shows that most breaches are the work of external threat agents. Whittling it down to IP theft doesn't change this, but it does take a dramatically different shape. Adding the percentages in Figure 1 yields an important distinction of IP-related breaches in our data set—both outsiders and insiders are often involved. Clearly, there is a great deal of collusion, which accounts for these ratios topping 100 percent.

We'll start with a look at the external agents. They often acted directly and maliciously, but also regularly solicited and/or aided others (insiders) to do their bidding. It's difficult to characterize the external agents involved (and clients often didn't seek attribution), but professional criminal rings, activist groups, competitors, and state-sponsored actors were identified or suspected. Those targeting IP are typically in a different class (in resources, skills, and determination) than the mainline fraudsters and script kiddies who perpetrate the bulk of cybercriminal activities across the Internet. While it is challenging to determine the true location of external adversaries (especially those with higher resources and capabilities), it's worth noting that over half of all intrusions originated from North America, about one-quarter from Asia, and 15% from Europe. Quite a few were unknown, and we'll leave the reader to make of these results what they will.

Figure 1. Threat agents by percent of breaches involving Intellectual Property theft



IP tends to reside deeper inside the organization under several layers of security, but insiders certainly know where it is and how to access it.

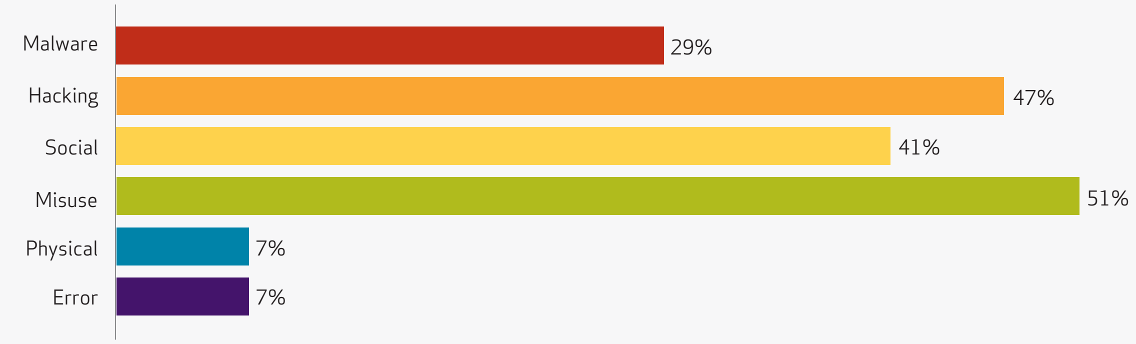
IP tends to reside deeper inside the organization under several layers of security, but insiders certainly know where it is and how to access it. For outsiders wishing to get at it with minimal risk and effort, recruiting insiders to participate often makes a good deal of sense. Regarding the types of insiders contributing to IP theft, regular employees (end users) accounted for the largest percentage (roughly two-thirds). They were followed closely by financial staff and executives, and (since we know you're wondering) system/network admins brought up the rear.

The take-home message here is that protecting IP from "them" is an incomplete and inadequate strategy. Understanding that "we" are sometimes our own enemy—and sometimes the enemy targets its own —is important to building good policy and practice for defending the crown jewels.

THREAT ACTIONS

Threat actions describe what the threat agent did to cause or to contribute to the breach. And when it comes to thieving IP, they're apparently willing to do quite a lot. Figure 2 and Table 2 illustrate well the diversity of methods employed to compromise this type of information.

Figure 2. Threat action categories by percent of breaches involving Intellectual Property theft

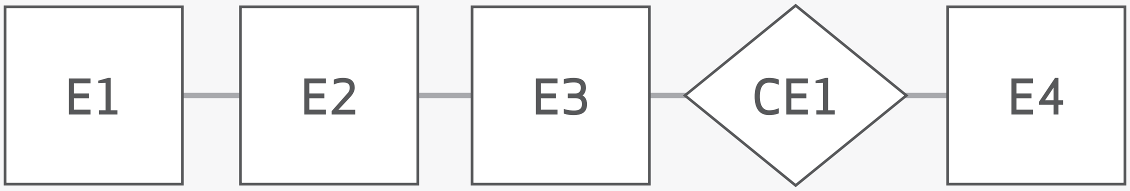


Whereas certain industries, such as Accommodation and Food Services[4], exhibit threat distributions that are heavily weighted toward hacking and malware, Figure 2 is remarkably more balanced. The de facto "smash and grab" scenario used to quickly exploit the payment processing infrastructure of many retailers and restaurants doesn't have a prayer of nabbing IP stored deep within the network. When simple automated attacks fail, determined adversaries will mix and match their methods until they find a successful combination. That may involve more advanced forms of hacking and malware and/or some good old-fashioned social engineering. Perhaps the services of an insider will be enlisted as well. The scenario originally discussed on pages 7 and 8 of the 2012 DBIR and republished here (Figure 3) is a fitting example of these multi-phased and multifaceted attacks. All of this results in a more diverse threat landscape, and, consequentially, the need for a more diverse control landscape.

When simple automated attacks fail, determined adversaries will mix and match their methods until they find a successful combination.

[4] The DBIR snapshot for the Accommodation and Food Services industry can be found at verizon.com/enterprise/travel.

Figure 3. Sample VERIS incident scenario



External agent sends a phishing e-mail that successfully lures an executive to open the attachment.	Malware infects the exec's laptop, creating a backdoor.	External agent accesses the exec's laptop via the backdoor, viewing e-mail and other sensitive data.	System administrator misconfigures access controls when building a new file server.	External agent accesses a mapped file server from the exec's laptop and steals intellectual property.
TE#280 External Social People Integrity	**TE#148** External Malware User Devices Integrity	**TE#130** External Hacking User Devices Confidentiality	**TE# 38** Internal Error Servers Integrity	**TE#4** External Hacking Servers Confidentiality

E = Event CE = Conditional Event TE# = Threat Event Number

Table 2 provides a more detailed list of common threat actions used to steal IP, and further underscores the diversity theme discussed above. Insiders abusing the system privileges granted to them to perform job duties take the top spot, and other forms of embezzlement and fraud make the list as well.

In terms of external breaches, the reader will find no mention of default or easily guessable credentials among the top ten. Instead, intrusions leverage stolen credentials to access internal systems while appearing legitimate to anyone who might be monitoring network activity. Keyloggers are often the means of capturing those credentials, while backdoors afford a stealthy mechanism for retaining access over the long term (and as will be shown later, it can be a very long term). System and network utilities, created for valid use by administrators, can also be used maliciously in the wrong hands. Squeezing into the top ten, SQL injection was used to pull records and upload malware as part of the chain of events leading to the compromise.

Table 2. Threat action varieties by percent of breaches involving Intellectual Property theft

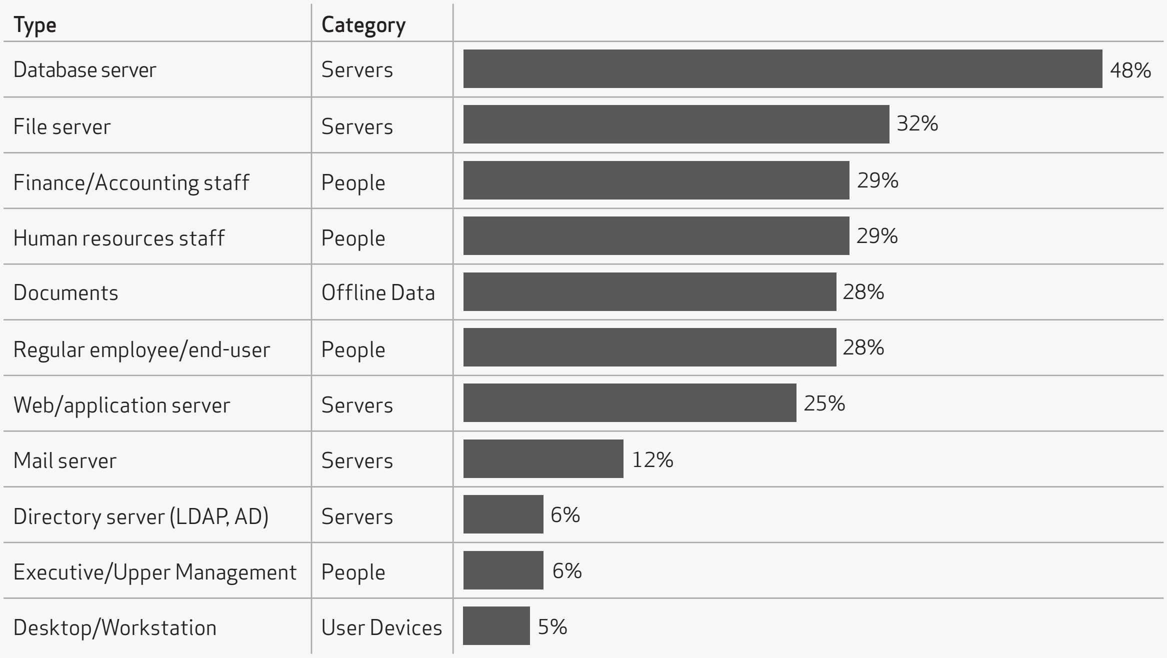
Rank	Variety	Category	Breaches
1	Abuse of system access/privileges	Misuse	45%
2	Use of stolen login credentials	Hacking	34%
3	Pretexting (classic Social Engineering)	Social	32%
4	Solicitation/Bribery	Social	28%
5	Embezzlement, skimming, and related fraud	Misuse	28%
6	Exploitation of backdoor or command and control channel	Hacking	25%
7	Backdoor (allows remote access / control)	Hacking	24%
8	Keylogger/Form-grabber/Spyware (capture data from user activity)	Malware	22%
9	Send data to external site/entity	Malware	22%
10	System/network utilities (PsTools, Netcat)	Malware	22%
11	Brute force and dictionary attacks	Hacking	20%
12	SQL Injection	Hacking	20%

Demonstrating that networks and applications aren't the only vectors of attack, social tactics exploiting the human vector factored prominently as well. Pretexting (the use of invented scenarios to deceive and/or manipulate) and solicitation contributed to the success of many incidents. This reinforces the importance of protecting the "carbon layer," which is a notoriously vulnerable and unpredictable component of the security model.

COMPROMISED ASSETS

To get a sense for what threat agents are targeting, and thus what's most in need of protecting, it's important to analyze the types of information assets affected by data breaches. Figure 4 records this information for incidents involving IP loss in our data set. In another interesting yet intuitive departure from run-of-the-mill cybercrimes, databases and file servers are the most often compromised. This is, quite simply, where most organizations store internal data and knowledge. Another popular form of long-term data storage, paper documents, also makes the list. This serves as a reminder that when we lock down file servers storing IP, we can't neglect to lock file drawers too.

Figure 4. Compromised assets by percent of breaches involving Intellectual Property theft*



Type	Category	
Database server	Servers	48%
File server	Servers	32%
Finance/Accounting staff	People	29%
Human resources staff	People	29%
Documents	Offline Data	28%
Regular employee/end-user	People	28%
Web/application server	Servers	25%
Mail server	Servers	12%
Directory server (LDAP, AD)	Servers	6%
Executive/Upper Management	People	6%
Desktop/Workstation	User Devices	5%

*Assets involved in less than 1% of breaches are not shown

There's an old adage that says "two people can keep a secret if one of them is dead," and looking at Figure 4, it's hard to argue with that bit of wisdom. Employees from the rank-and-file to upper-level executives were exploited in the process of obtaining organizational secrets. Some will find it odd that we treat people as assets, but in terms of processing, storing, and distributing information, they work similar to any other piece of hardware and software in the list. Plus, including people is yet another reminder that "wetware" is an asset that must be protected like any other.

Employees from the rank-and-file to upper-level executives were exploited in the process of obtaining organizational secrets.

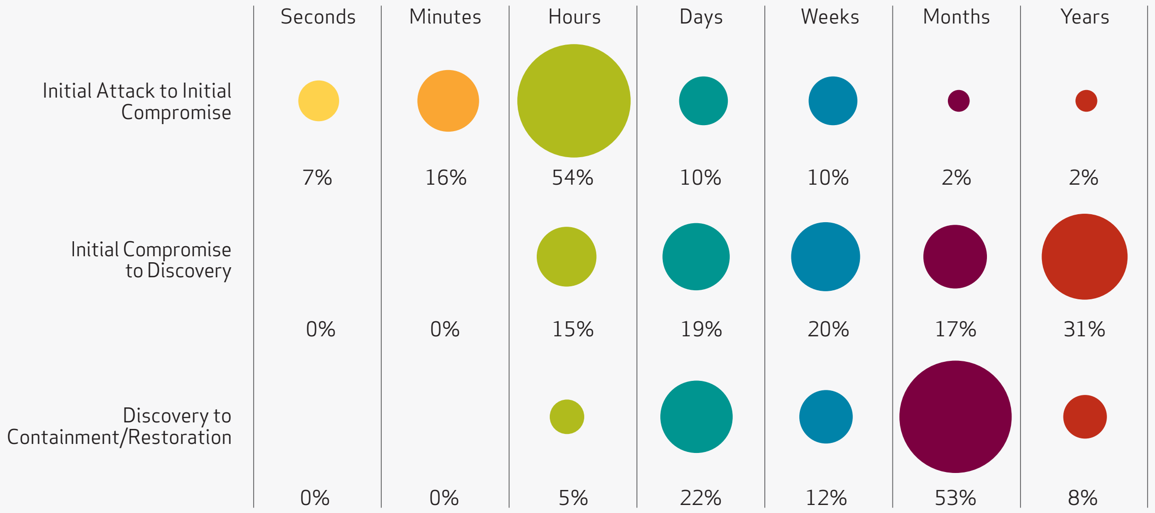
TIMELINE OF EVENTS

Response time is a good indicator of the maturity of an organization's security program. No one wants to be the victim of a breach, but if that unfortunate event arises, it's certainly better to know sooner rather than later, to limit exposure and take proper corrective measures. Among the major phases we consider in an event scenario are:

- **Initial Attack to Initial Compromise.** The time spanning from the first malicious action taken against the victim until an information asset is negatively affected.
- **Initial Compromise to Discovery.** The time spanning from when the first asset is negatively affected until the victim learns of the incident.
- **Discovery to Containment/Restoration.** The time spanning from when the victim learns of the incident until data is no longer actively exposed.

For a more complete accounting of incident scenario phases, please refer to the DBIR.

Figure 5. Timespan of events by percent of breaches involving Intellectual Property theft



We debated whether or not to present statistics for the "initial attack to initial compromise" phase in Figure 5 due to a high amount of unknowns. Instead of omitting potentially useful information, however, we'll just caveat it. In many cases, it was difficult to pinpoint a precise time when the attack began—especially since so many of these used human vectors, which don't record a timestamp in a log. Reviewing the numbers at face value shows a distribution clustered around "hours," and the tail to the right suggests IP thieves are willing to expend significant time and effort to gain that initial foothold into the victim.

Whereas our historical findings consistently show breach discovery timeframes in the "months" category, IP theft frequently takes years to discover.

The second row is simply fascinating. Whereas our historical findings consistently show breach discovery timeframes in the "months" category, IP theft frequently takes years to discover. Reasons for this are numerous, but the biggest among them is that the criminal usually dictates both the timeframe and method of discovery. When they begin using stolen data for fraud, the victim will then be notified of the breach by the payment card brands. Since IP is not used for post-breach fraud, this mechanism of discovery does not come into play. Instead, you look up a couple years later and wonder at the surprising similarity between your gizmo and the enhanced version your competitor just launched. The ironic truth is that without the help of the credit card companies and their comparatively mature and effective fraud detection mechanisms, we're left to our own devices. And the track record on that is not good.

To add insult to injury, it often takes quite a while before the breach is successfully contained. Once organizations realize that they've been victimized, it's crucial they mount a swift and competent response. But due to the complexity and longevity of many IP-related breaches, identifying all systems involved can be a real challenge. After remediating all (known) systems in scope, it's quite common that backdoors and other various hooks into the environment still exist. Thus, containment can become a drawn-out game of plugging holes and waiting for leaks to spring up elsewhere.

RECOMMENDATIONS FOR PREVENTING INTELLECTUAL PROPERTY THEFT

Because our dataset and, therefore our findings, evolve over time and encompass victims of different types, sizes and geographic locations, creating a single list of recommendations that work equally and effectively for all organizations is unrealistic. Our basic advice—beyond covering the security essentials—is to adopt a common sense, evidence-based approach to managing security. Learn what threats and failures most often affect organizations like yours, and then make sure your security posture puts you in a position to thwart them.

There is no silver bullet that can guarantee protection against IP theft. The diversity, complexity, and ingenuity of tactics preclude a one-size-fits-all solution. As our findings have shown, however, there are several common factors across successful attacks that warrant attention. Insider abuse—whether premeditated or requisitioned through trickery—is a favored method of filching IP. And if an insider won't cooperate, stealing their credentials will work almost as well. Short of that, brute-forcing or using SQL injection against web applications stands a good chance of success. However unauthorized access is accomplished, attackers will always want to expand and retain it, and that's where system utilities and backdoors come into play. Given all that, a few recommendations are provided below.

The diversity, complexity, and ingenuity of tactics preclude a one-size-fits-all solution.

Privileged Users

Trust but verify. Use pre-employment screening to eliminate the problem before it starts. Don't give users more privileges than they need (this is a biggie) and use separation of duties. Make sure they have direction (they know policies and expectations) and supervision (to make sure they adhere to them). Privileged use should be logged and generate messages to management. Unplanned privileged use should generate alarms and be investigated.

Training and Awareness

Increase awareness of social engineering: educate employees about different methods of social engineering and the vectors from which these attacks could arise. In many of our cases, we see users clicking on links they shouldn't and opening attachments received from unidentified persons. Reward users for reporting suspicious people, interactions, e-mail, or websites and create the incentives necessary for vigilance.

Stolen Credentials

Keeping credential-capturing malware off systems is priority number one. Consider two-factor authentication where appropriate. If possible, implement time-of-use rules, IP blacklisting (consider blocking large address blocks/regions if they have no legitimate business purpose), and restricting administrative connections (i.e., only from specific internal sources). Employing a "last logon" banner and training users to report/change passwords upon suspicion of theft also have promise.

Secure Development

Focus on application testing and code review. While SQL injection attacks are the most common, cross-site scripting, authentication bypass, and exploitation of session variables contributed to many of the network-based attacks. As with everything else, put out the fires first: even lightweight web application scanning and testing would have found many of the problems that led to the breaches we've analyzed. Next, include regular reviews of architecture, privileges, and source code. Incorporating a Security Development Life-Cycle (SDLC) approach for application development is recommended as well. Finally, help your developers learn to appreciate and write more secure code.

Log Monitoring and Analysis

Monitor and filter network egress traffic. At some point during the sequence of events in many breaches, something (data, communications, connections) goes out that, if prevented, could break the chain and stop the breach. By monitoring, understanding, and controlling outbound traffic, an organization will greatly increase its chances of mitigating malicious activity.

Enable application and network logs and monitor them. All too often, evidence of events leading to breaches was available to the victim but this information was neither noticed nor acted upon. Processes that provide sensible, efficient, and effective monitoring and response are critical to protecting data. However, don't just focus your logging efforts on network, operating system, IDS, and firewall logs but neglect remote access services, web applications, databases, and other critical applications. These can be a rich data set for detecting, preventing, and investigating breaches.

All too often, evidence of events leading to breaches was available to the victim but was neither noticed nor acted upon.

Define "suspicious" and "anomalous" (then look for whatever "it" is). This is admittedly vague, but—in truth—generalizing what this entails in order to prescribe something for everyone would counteract the point. Discover what is critical, identify what constitutes normal behavior, and then set focused mechanisms in place to look for "it" and sound the alert upon deviations from normality.

Change your approach to event monitoring and log analysis. Based on the timeline of many attacks, we believe that organizations would be better served to focus less on the "real-time" methods of detection, and more on "this-day" or "this-week" methods. Focus on the obvious things rather than the minutia. This need not be expensive; a simple script to count log lines/length and send an alert if out of tolerance can be quite effective. We're confident that this approach will reap benefits and save time, effort, and money.

To learn more about these findings or solutions to help your organization address similar concerns in your enterprise, contact your account manager or visit verizon.com/enterprise/security.

verizon.com/enterprise