InformationWeek
:: reports

Reports.InformationWeek.com

May 2013 $99

Next

The 8 Most Common Causes of Data Breaches

It seems as though not a day goes by without a headline screaming that some organization has experienced a data breach, putting the business — and its customers and partners — at risk. To keep your own organization out of the news, it's important to understand the most common causes of data breaches and what you can do to mitigate the threats they present.

By Fahmida Y. Rashid

Presented in conjunction with

SECURITY dark READING
Protect The Business Enable Access

Report ID: S6980513

TABLE OF CONTENTS

ABOUT US

InformationWeek Reports' analysts arm business technology decision-makers with real-world perspective based on qualitative and quantitative research, business and technology assessment and planning tools, and adoption best practices gleaned from experience.

OUR STAFF

Lorna Garey, content director; lorna.garey@ubm.com
Heather Vallis, managing editor, research; heather.vallis@ubm.com
Elizabeth Chodak, copy chief; elizabeth.chodak@ubm.com
Tara DeFilippo, associate art director; tara.defilippo@ubm.com

Find all of our reports at reports.informationweek.com.

Fahmida Y. Rashid
InformationWeek Reports

Fahmida Y. Rashid is an analyst who has covered networking and security for a number of years. Rashid was a senior writer covering security, core Internet infrastructure and open source at *eWEEK*. Rashid reviewed networking security software, hardware and services as an analyst at PCMag Labs. She was also a senior technical editor at CRN Test Center reviewing open source, storage and networking products from 2007 to 2008. Before setting out her journalism shingle, she was a technology consultant, first at PricewaterhouseCoopers and later with the Business Consulting Services group in IBM Global Services. She has worked in the trenches in help desk, QA tester, software and Web developer, and network administrator roles.

EXECUTIVE SUMMARY

Your organization's data is valuable — both to the organization and to any number of cybercriminals who are looking to do damage, make money, reap revenge, sabotage the business, get to your partners through your network … the list goes on and on, unfortunately. And not only are there numerous people and institutions that would like to get at your data, there are numerous ways for them to do so.

With that said, there are some common methodologies that cybercriminals use to infiltrate data systems, and knowing what those methodologies are is the first step to taking arms against them. In this *Dark Reading* report, we enumerate the most common types of data breaches, provide insight into how they're perpetrated and offer recommendations for heading them off.

The 8 Most Common Causes of Data Breaches — and How You Can Prevent Them

Lost laptops. Stolen password databases. Internal documents copied onto a USB drive.

Data breaches have dominated headlines recently. Whether it's nation-state spies intent on stealing information, cyber pranksters and hacktivists looking for attention, or cybercriminals out to make a buck, there are plenty of adversaries intent on breaking into networks and databases and carrying away whatever pieces of information they can grab.

"And from pubs to public agencies, mom-and-pops to multinationals, nobody was immune," the Verizon RISK Team writes in its "2013 Data Breach Investigations Report." Verizon investigators analyzed information from 621 data breaches and more than 47,000 security incidents in 2012 that the company or one of its 19 partner organizations had investigated on the behalf of customers.

All data is valuable to someone, and during the past two years, enterprises and consumers have increasingly learned just how vulnerable the systems storing personal and sensitive data happen to be. Weak passwords, malware, incorrect configurations, lax permissions … the list goes on. With each new headline, "a growing segment of the security community adopted an 'assume you're breached' mentality," Verizon RISK researchers write in this year's DBIR.

Figure 1

Most Data Breaches Come From the Outside

The biggest threat to organizations comes from external attackers. While large organizations may have more employees, the risk of a malicious insider does not increase.

- >> External: 92% (overall), 88% (SMB), 94% (large business)
- >> Internal: 14% (overall), 19% (SMB), 12% (large business)
- >> Partner: 1% (overall), 1% (SMB), 1% (large business)

Data: Verizon 2013 Data Breach Investigations Report

Motives for the data breaches are diverse. Hacktivists and those looking to make some money generally go after the low-hanging fruit — the insecure systems in the enterprise — to carry out their plans. Organized crime may be a bit more willing to spend the time going after better-protected systems in hopes of a bigger payoff. Then there are those targeting a specific individual or organization — these adversaries are stealthy and persistent enough to slowly chip away at defenses until they get what they are looking for.

Even as the list of victims gets longer, it's increasingly clear that some of these breaches could have been prevented. Of the breaches included in the report, 78% had initial intrusions Verizon's investigators rated as "low difficulty." Many of these attacks could have been prevented by adopting security controls, switching authentication schemes and adopting best practices, Verizon suggested.

In this *Dark Reading* report, we'll explore the most common causes of data breaches, the methods used by attackers and how organizations can improve their defenses to reduce the number of security incidents that hurt the bottom line.

Who Are the Attackers?

Not all data breaches are intentional or malicious. Losing a laptop at a conference isn't considered a data breach unless it contained unprotected sensitive customer or financial information. A university network administrator would be considered negligent for accidentally posting student information on an FTP server used to transfer university records, but it wouldn't be a breach until the server was publicly accessible.

Verizon's DBIR categorizes anyone involved in a data breach as one of the three types of threat actors: external, internal or partner.

As expected, a significant majority, or 92%, of security incidents and data breaches were the work of external parties. External actors include organized crime, state-affiliated hackers, activists and ex-employees. From a purely numbers viewpoint, there will always be more outsiders than insiders for a given organization. The Internet also gives criminals access to a "virtually limitless host of potential victims," the report says.

Even at 14%, insiders pose a significant threat. There are many reasons employees and trusted members of the organization may be considered a threat actor, including anger and frustration with the company, configuration mistakes coercion or just plain greed. IT staff and administrators aren't the only ones who can act against the organization; the report lists executives, managers, end users, cashiers, developers, call-center staff and even the maintenance crew as potential actors.

Partners, contractors, suppliers and other business entities that work with the organization but don't have the same level of privileges as employees are also a risk. External attackers

Figure 2

What Threat Actors Want

There is a strong co-relation between the type of actor and the type of data being targeted. Certain types of attacks are more common in certain industries than others. Organizations need to know which type of threat they are likely to face.

	Organized Crime	Nation State	Activists
Industry Targeted	Financial services, retail, food	Manufacturing, professional services, transportation	Information, public, services
Desired data	Payment card info, login credentials, financial accounts	Credentials, internal organization data, intellectual property & trade secrets, system configuration	Personal information, credentials, internal organization data
Common methods	Physical tampering, brute-force attacks, malware (information stealer, spyware)	Malware (backdoor, information stealing, password dumper, downloader), phishing, stolen credentials, command & control activities	SQL injection, stolen credentials, hacking, backdoor malware
Targeted equipment	ATM, POS equipment, database, desktop (endpoint)	Laptop, desktop, file server, mail server, directory server	Web applications, database, mail server

Source: Verizon 2013 Data Breach Investigations Report

S6980513/2

Offensive Cybersecurity

Offense is the new defense for private sector security professionals, some pundits would have you believe. Whether you call it "hacking back" or old-fashioned eye-for-an-eye retaliation, offensive security calls for profiling and, if possible, individually identifying an attacker and taking countermeasures to harm the attacker's systems. Governments have experimented with offensive security and have their own reasons and hesitations around pursuing it. For the private sector, though, it's a controversial approach that IT and business leaders should understand.

Download

could use weaker partner systems to piggyback into a target network, or the partner could have made a mistake as part of its management tasks. Only 1% of the breaches Verizon reported involved a partner in some way.

What Is Getting Breached?

While the "who" is important, defenders and investigators are also interested in the question of "what" the attackers are going after. Verizon found that 71%, or nearly three-quarters, of the incidents investigated in its report targeted user endpoint devices. A little over half, or 54%, of the breaches involved at least one compromised server.

"The end user device continues to be the weakest link in the security chain," says George Tubin, a security strategist with Trusteer.

A full 75% of the incidents were considered opportunistic attacks, indicating that even with the increased headlines about highly sophisticated targeted attacks, most of the time the attacker doesn't really care who the victim is. Rather, the victim was compromised because it had a weakness the attacker knew how to exploit. Nearly all the opportunistic attacks were financially motivated, according to the report.

There was a "definite relationship" between industry and attack motive, the Verizon RISK Team writes. Retailers are more likely to see financially motivated attackers going after payment card information, while manufacturers are likely to be faced with attacks targeting intellectual property.

"Any attempt to enforce a one-size-fits-all approach to securing our assets may result in leaving some organizations unprotected from targeted attacks while others potentially overspend on defending against simpler opportunistic attacks," states the report.

Causes of Data Breach

While Verizon investigators cautioned against trying to treat all the breaches in the same way, they identified several ways in which organizations have been compromised. Understanding these categories can help organizations figure out how best to boost their defenses.

Several of the most common attack methods in the report fall into two broad categories: hacking and malware. The report identifies hacking as the most common method, at 52%, followed by malware, at 40%, and physical attacks — such as adding skimming hardware on ATMs — at 35%. Social engineering is also a serious problem, at 29%. "Misuse," which includes activities such as privilege abuse and using unapproved hardware and correlated strongly with insider attacks, was observed in 13% of the breaches. User error rounded out the list with 2%.

"Treating our adversaries as random and unpredictable is counterproductive. We may be able to reduce the majority of attacks by focusing on a handful of attack patterns," Verizon researchers write in the report.

Following are eight ways that enterprise systems and data are being targeted.

1. Weak and Stolen Credentials, a.k.a. Passwords

Hacking remains the single biggest cause of data breaches, but the vast majority of the

attacks don't depend on finding vulnerabilities in the application or network protocol to tunnel through. For years, experts have warned about the risks of relying on weak credentials to restrict who has access to the data, and this is still a problem.

About 76% of network intrusions involved weak credentials, according to Verizon's data breach report. Authentication-based attacks, which includes guessing passwords, cracking using specific tools or trying out passwords from other sites on the target system, factored into about four of every five breaches that was classified as a hacking incident in 2012, Verizon says.

"Even with all the hype around APTs and hacktivists last year, an organization is still far, far more likely to be breached opportunistically, and the most likely vector will be weak or stolen authentication credentials," says Ross Barrett, senior manager of security engineering from Rapid7.

Stolen passwords played a role in 48% of the data breaches that involved hacking, Verizon found. This could have been accomplished by using stolen password lists from previous data breaches, keylogging malware or phishing attacks.

If that number isn't eye-popping enough, Verizon estimated that 80% of data breaches would have been stopped or forced to change tactics if a "suitable replacement" (such as multifactor authentication) to passwords had been used.

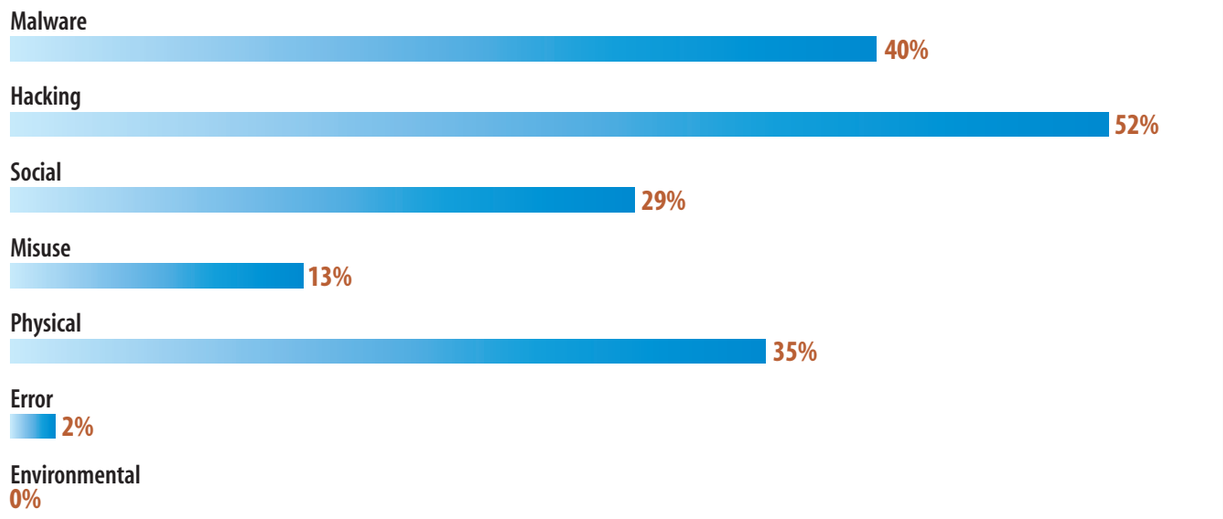
"We could use these statistics to overthrow single-factor passwords: the supreme ruler in the world of authentication," the Verizon report says.

Brute-force attacks (34% of data breaches

Figure 3

Most Common Attack Methods

Malware and hacking are the most common methods used in data breaches. Many incidents require both malware and hacking in a one-two combo. Misuse primarily applies to insider incidents. Social engineering has quadrupled since 2011.



Source: Verizon 2013 Data Breach Investigations Report S6980513/3

involving hacking) disproportionately affect smaller organizations, but larger organizations are still vulnerable. People need to realize that using the same passwords across multiple services makes all the services vulnerable: If one account is cracked, all the others become vulnerable. Even if passwords are stored securely, available cracking tools have made it pretty easy to decode the original password, especially if the selected string is not very long or complex. Attackers can also brute-force passwords just by trying some of the most common passwords (such as "password").

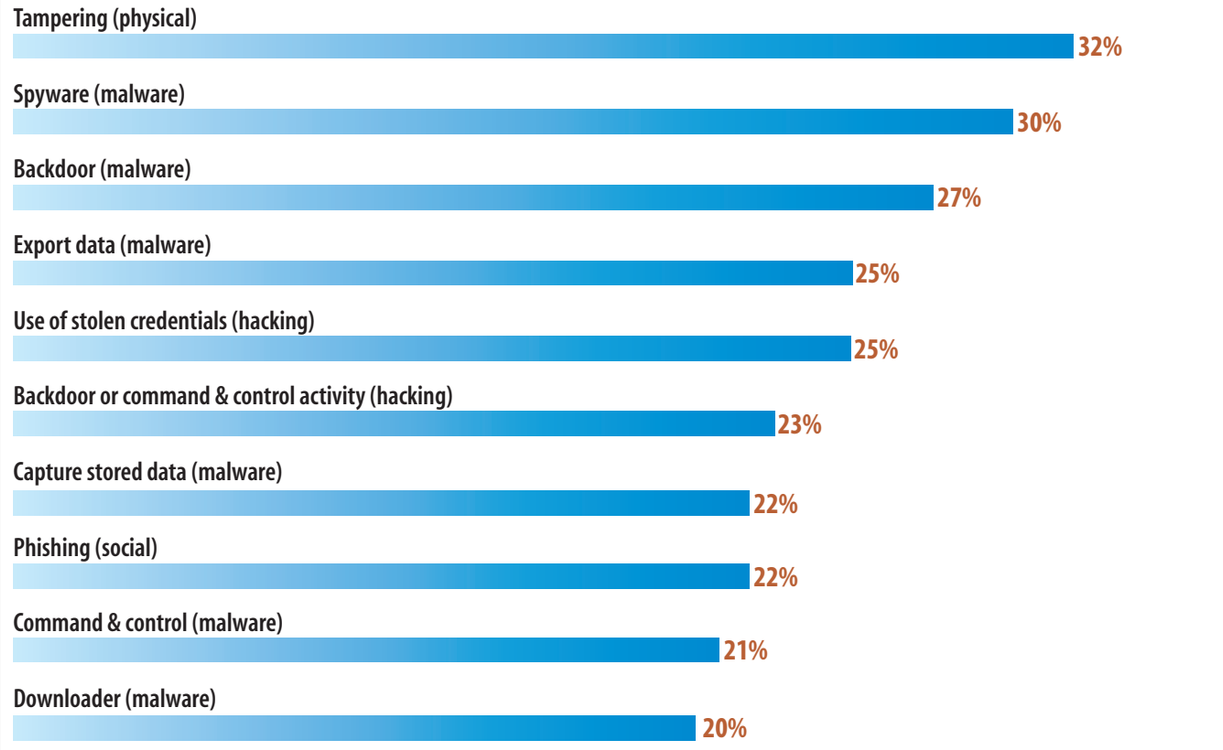
"Vanilla password cracking — guessing or reusing credentials — is by far the most popular way to pass through the security gate," says Andy Green, a technical content specialist with Varonis Systems. "You can get a lot of bang for the buck by simply changing default passwords for all purchased software products and enforcing password standards for employees."

Verizon investigators point out that the shortcomings of using passwords are well-known, but they acknowledge that it hasn't

Figure 4

Top 10 Attack Methods Used

It's one thing to say that malware and hacking are the most common causes of data breaches. But what exactly are attackers doing?



Source: Verizon 2013 Data Breach Investigations Report

S6980513/4

been an easy problem to fix. However, attitudes may be changing. A survey from the Ponemon Institute recently looked at consumer attitudes toward authentication and found that 65% said they did not trust systems or websites that relied only on passwords. The same survey found that 70% of respondents would favor using mobile devices or other forms of identity verification instead of just relying on passwords.

Internet consumers in the survey were "more aware and willing to try new methods of online security than we expected," says Larry Ponemon, founder and head researcher at Ponemon Institute.

Attacks on SSH are "the most alarming of all attacks" because cryptographic keys and digital certificates establish trust for every online business, Kevin Bocek, VP of product marketing at Venafi.

2. Back Doors, Application Vulnerabilities

Considering that Verizon's system identifies more than 40 types of hacking, the fact that nearly all the hacking activity was accounted for by five methods is "remarkable," the researchers wrote. Along with use of stolen credentials and brute-force methods, both of which deal with the issue of weak credentials, other common hacking actions include the use of back doors (44%) and SQL injection (8%). Exploiting buffer overflow vulnerabilities made the top 10 common hacking actions, but was observed in only 1% of the incidents.

"Security teams have to use tools that sift through tens or hundreds of thousands of vulnerabilities continuously, finding the most likely attack routes and the vulnerabilities that need to be blocked to prevent the breach," says Gidi Cohen, CEO and founder of Skybox Security.

Attacks exploiting vulnerabilities in Web applications increased from previous years but are no longer the leading attack vector among larger organizations, Verizon found.

Back doors refer to threat actors gaining access to an application or the network by finding and exploiting a back door, and not relying on malware that opened a back door on the infected system. This attack vector appears quite popular in state-sponsored targeted campaigns where the attackers set up the back door to gain initial access and then use remote shell services such as Secure Shell (SSH) and remote procedure calls to move around the network.

Attacks on SSH are "the most alarming of all attacks," because cryptographic keys and digital certificates establish trust for every online business, says Kevin Bocek, VP of product marketing at Venafi. They are also costly: Another Ponemon Institute survey estimated that organizations are at risk of losing $398 million from attacks on failed key and certificate management. Only half of the organizations in the Ponemon survey knew how many keys and certificates were in use. If the organization doesn't have strong visibility over its certificates and SSH keys, it won't be able to detect when attackers are bypassing the controls and moving around the network.

In nearly 78% of breaches, the method used to initially compromise the system was simple enough that an average user could have accomplished the task with little to no special resources, using basic methods and with

some automated tools and scripts, Verizon found. There is no need for attackers to "fire a guided missile at an unlocked screen door," since the simple methods work just as well without the effort, Verizon found.

Verizon recommends that organizations look at the 20 critical security controls as defined by the Consortium for Cybersecurity Action. Most of the common threat actions could be addressed by the controls, such as performing continuous vulnerability assessments and remediation to find vulnerabilities, checking ports and applying patches. The controls also include application testing and code reviews.

3. Malware

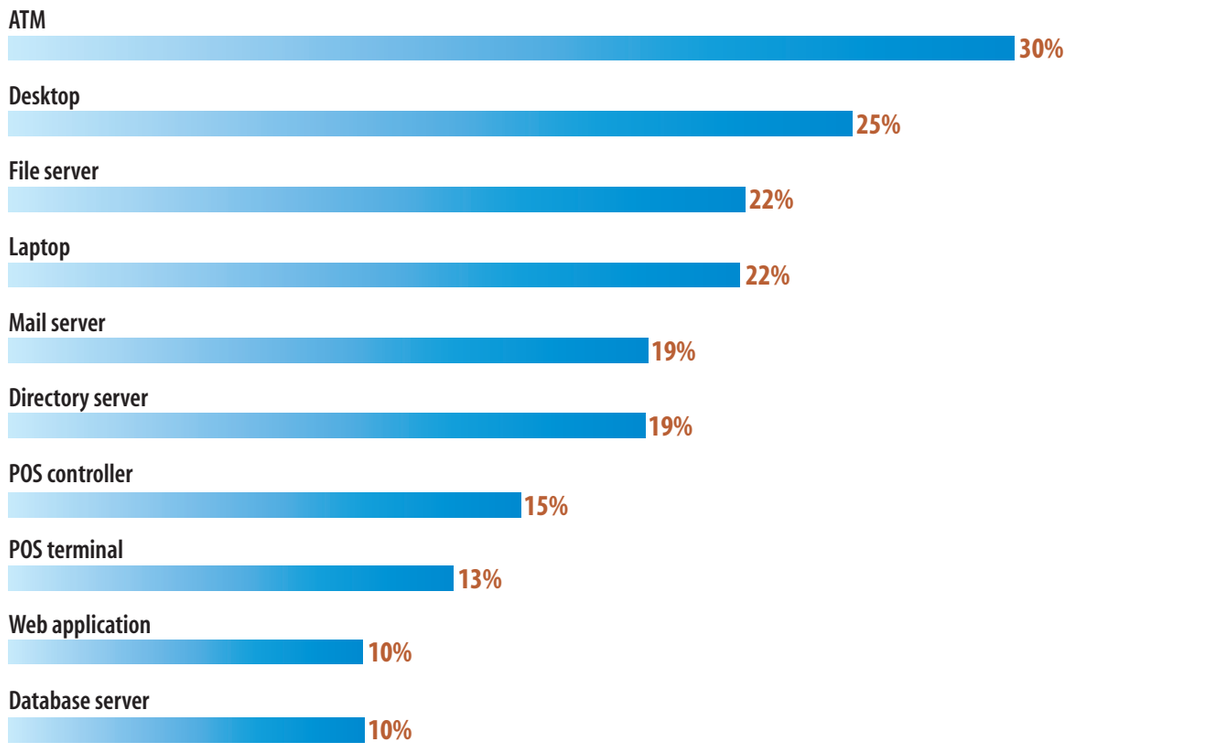
Malware remains a serious problem for data breaches. While there are sophisticated cyberweapons such as Stuxnet and Flame out there, most malware variants are not that fancy.

Directly installed malware made up about 74% of all the cases involving malware, the Verizon report found. Strategic Web compromises, popularly known as watering hole

Figure 5

What Gets Hacked

End user devices are the most frequently targeted in data breaches, but servers are regularly targeted because they generally contain all the data that is of interest.



Source: Verizon 2013 Data Breach Investigations Report S6980513/5

attacks, which utilized drive-by exploits to download malware onto victim computers, were more prevalent among larger organizations in both espionage and financially motivated attacks, Verizon found.

Spyware such as keyloggers and form-grabbers were the most common forms of malware (75%), the study found, but back doors (66%), information stealers, command-and-control malware (51%), password dumpers (45%) and rootkits (39%) were also prevalent in the top 10 malware types in the report.

Spyware dominated financially motivated breaches. For example, it was used to capture data from payment cards swiped at point-of-sale terminals, as well as to intercept account credentials typed into online banking sessions. Spyware was also observed in espionage incidents, where it grabbed screen shots of applications and stole user credentials.

The spyware problem is different than the weak credentials problem identified earlier: It doesn't matter how strong or complex a password is if the keylogger steals the entire thing. As a result, it's important for organizations to detect compromised accounts quickly, says Chris Petersen, CTO of LogRhythm. Behavioral analysis provides real-time detection of compromised accounts so that IT can automatically disable the account and shut down attack activity, he adds.

Back doors, command-and-control and data capture/export malware remained highly popular in cybercrime attacks. Verizon investigators also highlighted the popularity of ransomware attacks against the small business. The risk of ransomware could be reduced by ensuring that remote access products such as Microsoft's Remote Desktop Protocol and VNC are patched regularly, keeping all systems and software up to date with the patches and anti-malware protection, and making sure backups are correctly running so data can be successfully restored without paying a ransom.

While the majority of malware infections were direct-install, malware distributed via email attachments and embedded links also increased. Email attachments were predominantly used in espionage cases, while embedded links were primarily used in financially motivated attacks.

4. Social Engineering

While breaches involving some form of social engineering accounted for only a third of the cases in Verizon's data set, investigators noted a "big upswing" in these types of attacks. Phishing was by far the most predominant form of social engineering, accounting for 77% of these cases, compared with bribery, at 12%. Other methods included extortion (4%), pretexting (3%) and influencing users (2 %).

While phishing wasn't unusual in financially motivated attacks, Verizon investigators found that state-affiliated espionage was the main driver for phishing. There have been multiple cases of attackers sending employees of a targeted organization a convincingly crafted email with a malicious attachment or linking to a malicious site. Either clicking on the link or opening the attachment could give the at-

tacker "the keys to the company's intellectual property kingdom," Verizon writes in its report.

"Thirty years ago, phone books used to be the only way to easily glean personal information," but all that has changed with social networking sites exposing more information online, says Jim Butterfield, CISO of HBGary. Attackers can use online sources of information, frequently provided by the victims themselves, to find out when employees are traveling, interviewing for a new job or frustrated at work.

"All of this information can be used to either reach out to potential insider threats or to gain access to an account and your network," Butterfield says.

Organizations need to focus on user training to teach employees to understand what social engineering attacks look like and review social media policies to make sure the accounts are managed responsibly. Verizon cited a different study conducted by Herndon, Va.-based ThreatSim, which found that an attacker has a better-than-50% chance of getting at least one click just by sending three phishing emails. There's no need to flood the organization with the phishing mail — sending eight to 10 messages almost guarantees that at least one employee will open the attachment or click on link, ThreatSim found.

Pretty much anyone can be targeted, from system administrators to call center staff to a cashier to a manager. Executives and managers are "sweet targets" because they have access to sensitive and proprietary information. Their higher public profiles also makes it easier to find information to craft social engineering attacks.

"We all know how much they love .ppt and .pdf attachments," the investigators write.

Just having employees recognize and report suspicious occurrences and having the IT team monitor outbound traffic for communications with malicious IP addresses "could be some of the most effective means of discovering a breach," according to the report.

5. Too Many Permissions

Incorrectly managing access to applications and different types of data can result in employees being able to view and transport information they don't need for their jobs. Role-based access control and a rights matrix enable organizations to put controls around what users can do and what information they can access, says Paco Hope, a principal at Cigital. Correctly implementing authorization is something that's frequently overlooked, but it's fundamental.

Verizon found that two-thirds of breaches involved data stored or "at rest" in databases and file servers. Organizations should review user privileges and harden databases and file servers to prevent unauthorized access to the data — or at least slow an attacker down, according to the report. The 20 critical controls address some ways to restrict user access, Verizon notes.

6. Insider Threats

Abusing user privileges is only one type of threat insiders pose. While employees may be looking at databases they don't need for their job and copying or sharing with unauthorized parties, the top three varieties of

misuse in Verizon's study were privilege abuse, embezzlement and the use of unapproved hardware.

A big problem with insider threats appears to be the fact that employees think they are entitled to the data. A Ponemon survey on insider threats earlier this year found that employees think it's acceptable to take and use intellectual property when they leave the company. About 62% said it was acceptable to transfer work documents to personal devices, and 56% did not believe it was wrong to use trade secrets from a former employer at a competitor.

To make matters worse, organizations aren't always disabling access as soon as employees leave the company. "If you take them off your payroll, take them out of your systems, too," states the Verizon report.

7. Physical Attacks

Physical attacks, which accounted for 35% of cases the Verizon RISK team investigated in 2012, included actions that required the attacker to be in the proximity of the compromised system. The most common physical data breach in 2012 was ATM skimming, where attackers installed card readers to download all track data from payment cards or tampered with point-of-sale devices.

Tampering was the most common type of physical data breach, at 91%, followed by surveillance-based breaches, at 9%. Stolen user devices containing sensitive data or data stolen using modified POS devices accounted for only about 8% of these cases. The majority of these attacks occurred in public places.

Verizon recommends network segmentation, securing configuration settings and controlling administrative privileges as just some of the ways organizations can protect their physical devices.

8. Improper Configuration, User Error

The Verizon DBIR didn't have a lot of information about breaches that were the result of a mistake in configuration or user error, which makes sense because "organizations rarely ask a third party to investigate incidents resulting from mundane mistakes or glitches," the investigators wrote. It's also tricky to define what constitutes an error. While the first inclination would be to tag a database having a blank password as an error, if the organization doesn't have fundamental security processes or standards already in place to forbid that and detect it when it happens, that's a serious problem and not just an error, the investigators note. A server misconfiguration that publishes private data to a public website, or emails with sensitive data being sent to the wrong recipient, would be regarded as an error.

"Breaches are a multifaceted problem, and any one-dimensional attempt to describe them fails to adequately capture their complexity," states the report.

Putting Security in Context

The Ponemon Institute found that, on average, data breaches cost organizations in the United States $194 per compromised record, and total organizational costs exceed $5 million.

The question about the costs to an organization after a data breach is an interesting one.

Some of the costs — remediating the issue and recovering systems — do not vary if the breach is detected the next day or several weeks later. However, others — such as the value of the data that was stolen, regulatory fines and brand reputation — rise exponentially the longer the breach remains undetected. Organizations need to focus on speeding up the time to detection so that less information is leaked out, Verizon's report says.

Some of the recommendations in the Verizon report include eliminating unnecessary data, ensuring and verifying that essential controls are implemented and being followed, as well as collecting and sharing tactical threat intelligence with peers and other public agencies.

Cyber attack prevention must begin with strong and effective endpoint protection, Trusteer's Tubin says.

Most organizations should implement most, if not all, 20 of the critical security controls, Verizon recommends. The controls aren't intended to be a list of must-do steps that will stop all data breaches, as none is intended to act as primary risk mitigation. How the controls should be implemented will depend on the organization's size, budget and business needs.

But above all, organizations need to take time to understand the threat landscape as it applies to them and their industry, and make decisions accordingly. Organizations generally have the tools, states the Verizon report; "it's selecting the right ones and using them in the right way" that is a challenge.

MORE LIKE THIS

Want More Like This?

InformationWeek creates more than 150 reports like this each year, and they're all free to registered users. We'll help you sort through vendor claims, justify IT projects and implement new systems by providing analysis and advice from IT professionals. Right now on our site you'll find:

How Attackers Choose Which Vulnerabilities to Exploit: In the increasingly complex world of information security, it's important for security professionals to be able to understand not only how their organization's systems and data may be compromised but why. In this *Dark Reading* report we examine why certain vulnerabilities are exploited, by whom and with what. We also provide recommendations for getting out in front of hackers by using some of the same tools and strategies they do.

Assessing Risk and Prioritizing Vulnerability Remediation: Vulnerability remediation is a never-ending process, but, even so, security pros can't plug every hole in every asset and application. The key is to determine which vulnerabilities are most likely to be exploited and the effects such exploits would have on the business. To do this, security pros must know the business and its technology usage and needs intimately, a process that must involve stakeholders across the organization. In this report, we recommend the steps that should be taken to determine the risk of vulnerabilities and the lengths to which remediation can and should go.

Finding Vulnerabilities by Attacking Your Own Environment: Vulnerability scans are valuable, but you have to think and act like a hacker if you want to truly understand the ways in which your organization could be compromised. In this report, *Dark Reading* recommends the tools and methodologies that can be used to test your organization's security.

PLUS: Find signature reports, such as the *InformationWeek* Salary Survey, *InformationWeek 500* and the annual State of Security report; full issues; and much more.