

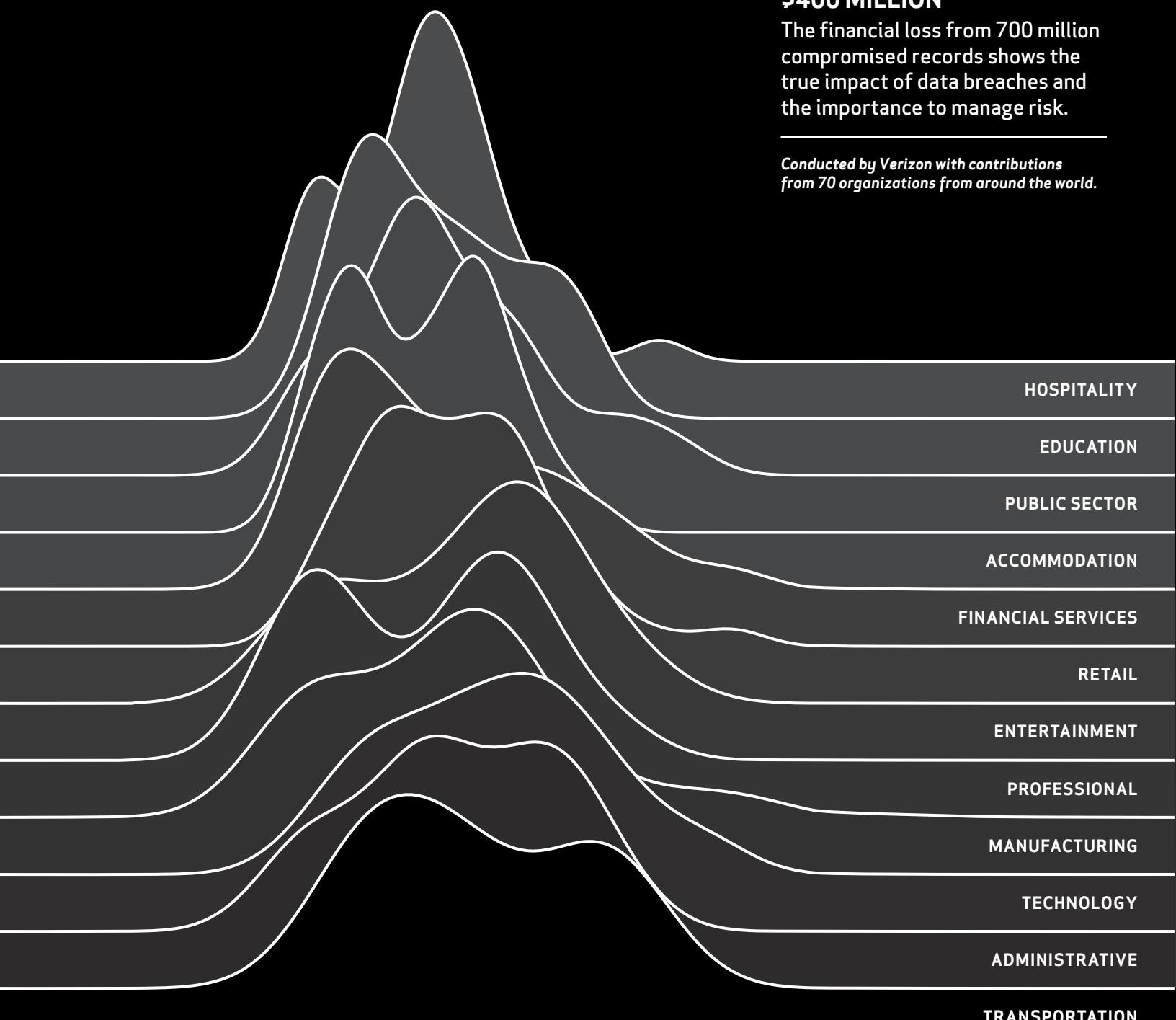


2015 DATA BREACH INVESTIGATIONS REPORT

\$400 MILLION

The financial loss from 700 million compromised records shows the true impact of data breaches and the importance to manage risk.

Conducted by Verizon with contributions from 70 organizations from around the world.



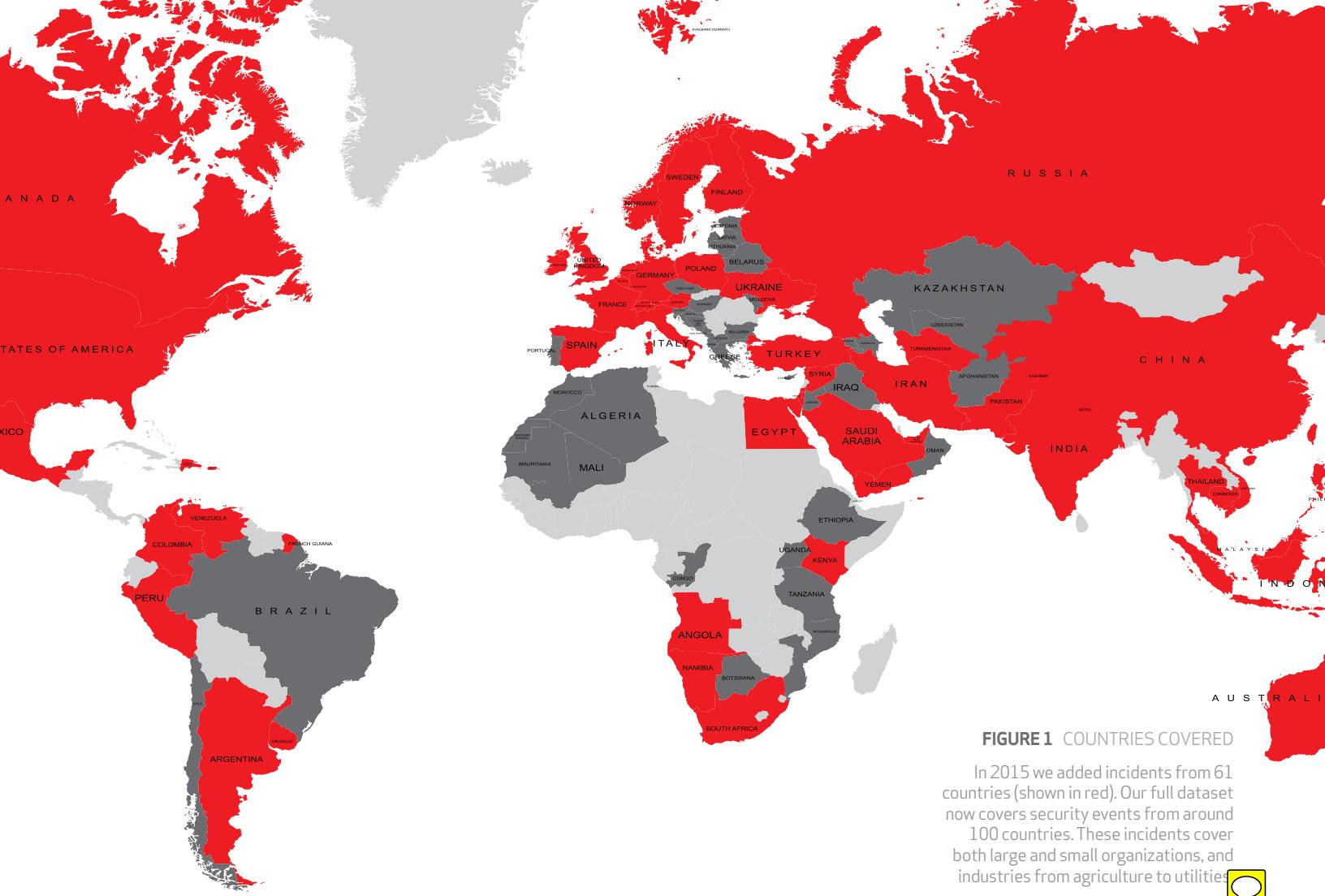


FIGURE 1 COUNTRIES COVERED

In 2015 we added incidents from 61 countries (shown in red). Our full dataset now covers security events from around 100 countries. These incidents cover both large and small organizations, and industries from agriculture to utilities.

THE 2015 DBIR

Why data security should matter to you

Protecting your organization from a data breach could save your organization hundreds of millions of dollars and help maintain customer loyalty and shareholder confidence.

Data security isn't something that should be left to the IT department. It's so important that it should matter to leaders, and indeed employees, from all functions.

The motives for attacks are varied: attackers may be looking for payment card data or sensitive commercial information, or simply to disrupt your business. And the methods of attack are becoming increasingly sophisticated — often involving a combination of phishing, hacking, or malware.

And then there's the staggering speed with which attackers can breach your defenses — it can take just seconds. But while attackers don't take long to compromise a system, in many cases it takes organizations months or even years to discover that they're a victim.

70
law enforcement agencies
and IT security companies
supplied data

2,122

data breaches analyzed

79,790
security incidents
classified

The Verizon 2015 Data Breach Investigations Report (DBIR) provides a detailed analysis of almost 80,000 incidents, including 2,122 confirmed data breaches. This summary covers some of our key findings.

New opportunities have emerged

Does the increased use of mobility and the Internet of Things (IoT) leave you more open to attacks on your data and systems?

We found that Android is the most vulnerable mobile platform, with malicious activity centered on malware — usually resource-wasting infections. But the incidence is still very low.

There have been few security incidents involving machine-to-machine (M2M) devices. But that doesn't mean you should ignore this area when planning your defenses — make sure you have robust access controls and encrypt sensitive data.

Old techniques are still a threat

Phishing remains popular with attackers. Campaigns have evolved to include the installation of malware as the second stage of an attack. Our data suggests that such attacks could be becoming more effective, with 23% of recipients now opening phishing messages and 11% clicking on attachments. It gets worse. On average, it's just 82 seconds before a phishing campaign gets its first click.

Across the 20,000 organizations we looked at, there were 170 million malware events intercepted. 70-90% of those were unique to a single organization. We're not talking about malware that is written to target a particular victim — although we've seen that too. We're referring to hackers introducing simple modifications to the code each time they use it. This changes the identifying signature that traditional anti-virus products look for, enabling the malicious code to get through and compromise systems.

Old vulnerabilities remain open

We found that ten vulnerabilities accounted for almost 97% of the exploits in 2014. The other 3% consists of 7,000,000 other vulnerabilities. Most attacks exploited known vulnerabilities where a patch has been available for months, often years. Of the vulnerabilities detected in 2014 we found more dating back to 2007 than from any year since.

Familiar patterns remain

Last year we identified nine incident patterns that cover most of the challenges you're likely to face. This year, those patterns covered 96% of all incidents. And the news gets better. In your industry, the majority of threats are likely to be covered by just three of these patterns. By using our nine incident classification patterns, you can effectively prioritize your efforts and build firm foundations for your defenses.

Adding up the costs

Organizations are constantly asking us to put a figure on the cost of breach to help them demonstrate the value that they are delivering and justify their data security budgets. This year, for the first time, the DBIR shows you what costs you can expect to incur if you fail to protect your data.

Other models tend to over-simplify the cost of a breach. We used actual cyber-liability insurance claims data to develop a more robust model that accounts for the uncertainty of costs as the number of records involved increases.

Using this model we can say, with 95% confidence, that the average loss for a breach of 1,000 records will be between \$52,000 and \$87,000 — \$52-\$87 per record. In contrast, the average loss caused by a breach affecting 10 million records will be between \$2.1 million and \$5.2 million — \$0.21 to \$0.52 per record.

23%

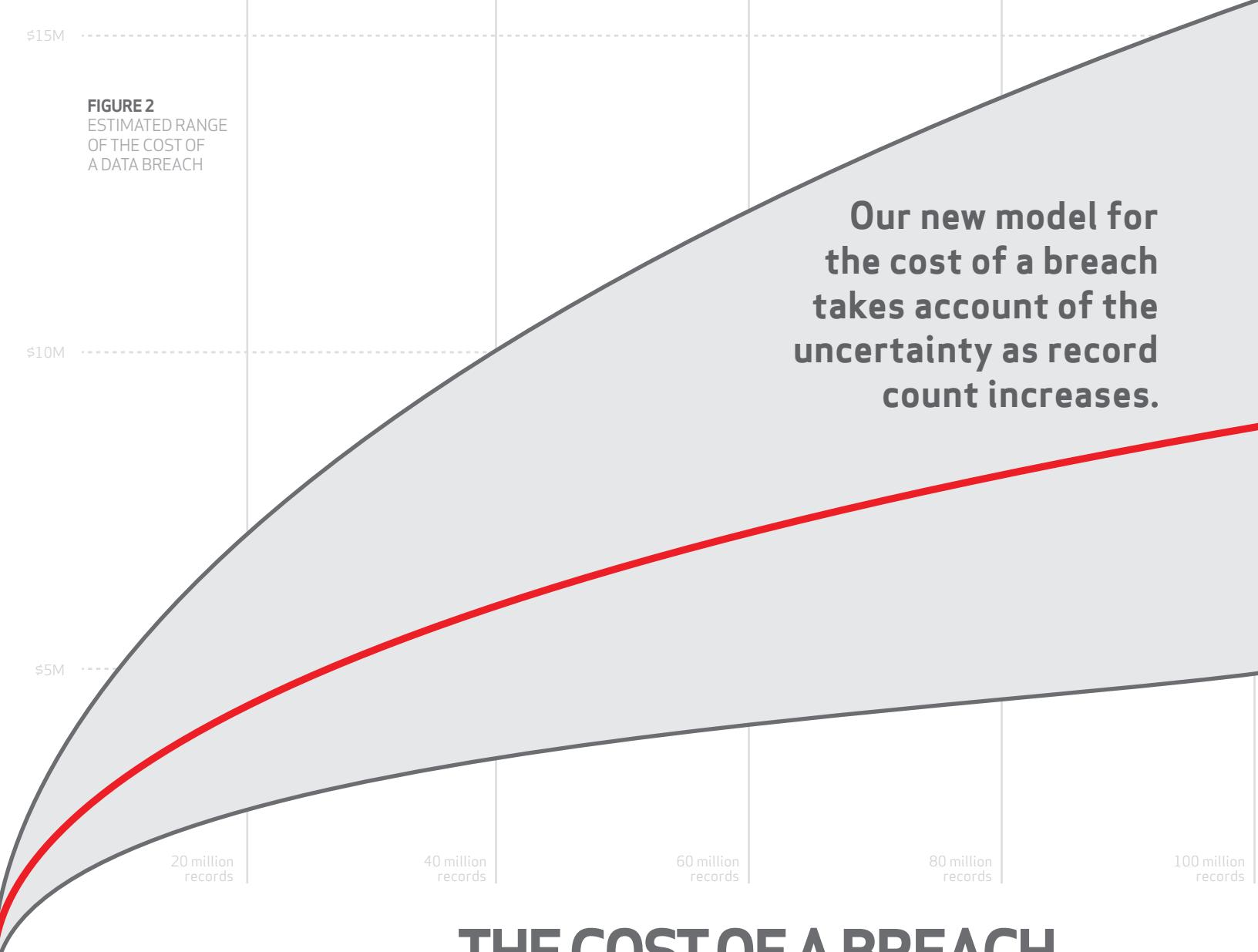
We found that in the last year, 23% of recipients opened phishing messages and 11% clicked on attachments.

96%

Last year we reported that 92% of the incidents that we'd seen over 10 years fitted into just nine patterns. While we saw many changes in the threat landscape in the last 12 months, these patterns still covered the vast majority of incidents (96%)

FIGURE 2
ESTIMATED RANGE
OF THE COST OF
A DATA BREACH

Our new model for
the cost of a breach
takes account of the
uncertainty as record
count increases.



THE COST OF A BREACH

\$254

The expected cost per record for breaches involving 100 records is \$254.

9¢

For breaches involving 100 million records, that figure drops to just \$0.09 — though of course the total cost is much higher.

How much does a data breach cost? We can now give you the most accurate picture yet of the costs you could incur if you fail to protect your data.

We've analyzed data on almost 200 cyber-liability insurance claims where there was a data breach. This has enabled us to bring you what we believe is the most accurate picture of the financial risk of a data breach currently available.

Beyond the average

Following the model used by other analysts, we started by working out an average cost per record. This was just \$0.58 — a lot less than other estimates based on survey data. But when we applied this to our examples of actual costs, it was clear that it didn't provide a very accurate estimate.

The cost of breach does not follow a linear model. In reality, the cost per record falls as the number of records lost increases. This means that when using an average, the variance grows greater as the number of records grows — and we wanted our model to cover a wide range of incidents, including those where more than 100,000 records were stolen.

So instead of using a simple average, we modeled how the actual cost varies with the number of records. We believe that this provides a much more accurate and reliable indicator.

And our model can be used to estimate the cost for breaches experienced by all organizations.

We found that company size has no affect on the cost of breach.

The headline-making losses reported by larger organizations can be explained by the fact that these involved the loss of more records. Breaches with a comparable number of records have a similar cost, regardless of organization size.

The best model available

We calculated an expected cost of breach of \$25,445 for 100 lost records (\$254/record), rising to almost \$9 million for the loss of 100 million records (\$0.09/record). But of course, the true cost of breach depends upon much more than just the number of records lost.

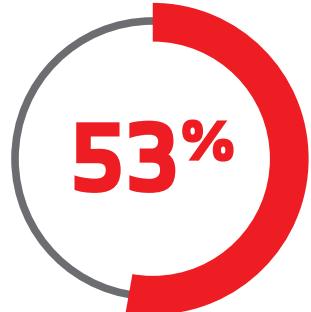
One of the most significant factors is the type of data lost, which can be anything from payment card details to medical records. To provide an accurate picture of the likely cost of a breach we need to look at a range, not just a single figure.

The table below shows the limits of two ranges around our expected figure, these are the 95% confidence intervals for the average and a single event — this is also shown on the chart on the left. The narrower band is for the average of multiple incidents involving the same number of lost records and the outer range is for any single incident.

So, for example, our model states that the loss for a breach involving 1,000 records will be between \$3,000 and \$1.5 million. This is a wide range as it has to cover many kinds of outlier. If we look at the average cost of a breach of this many records, we can say that it will fall between \$52,000 and \$87,000.

What does this mean for me?

The costs of a breach can far outweigh the effort and resources required to keep your business secure. We hope that this model helps you when you're trying to explain the financial implications of a data breach to your organization.



Our analysis suggests that 53% of the variation in the cost of a breach can be accounted for by the number of records lost. The rest is likely to be down to a number of factors, including preparedness.

FIGURE 3 COST OF A BREACH BREAKDOWN

| Records | Prediction (lower) | Average (lower) | Expected | Average (upper) | Prediction (upper) |
|-------------|--------------------|-----------------|-------------|-----------------|--------------------|
| 100 | \$1,165 | \$18,118 | \$25,445 | \$35,734 | \$555,664 |
| 1,000 | \$3,115 | \$52,258 | \$67,480 | \$87,136 | \$1,461,728 |
| 10,000 | \$8,283 | \$143,362 | \$178,960 | \$223,396 | \$3,866,367 |
| 100,000 | \$21,905 | \$366,484 | \$474,606 | \$614,627 | \$10,283,189 |
| 1,000,000 | \$57,609 | \$892,356 | \$1,258,669 | \$1,775,353 | \$27,500,090 |
| 10,000,000 | \$150,687 | \$2,125,897 | \$3,338,026 | \$5,241,279 | \$73,943,954 |
| 100,000,000 | \$392,043 | \$5,016,243 | \$8,852,541 | \$15,622,747 | \$199,895,081 |

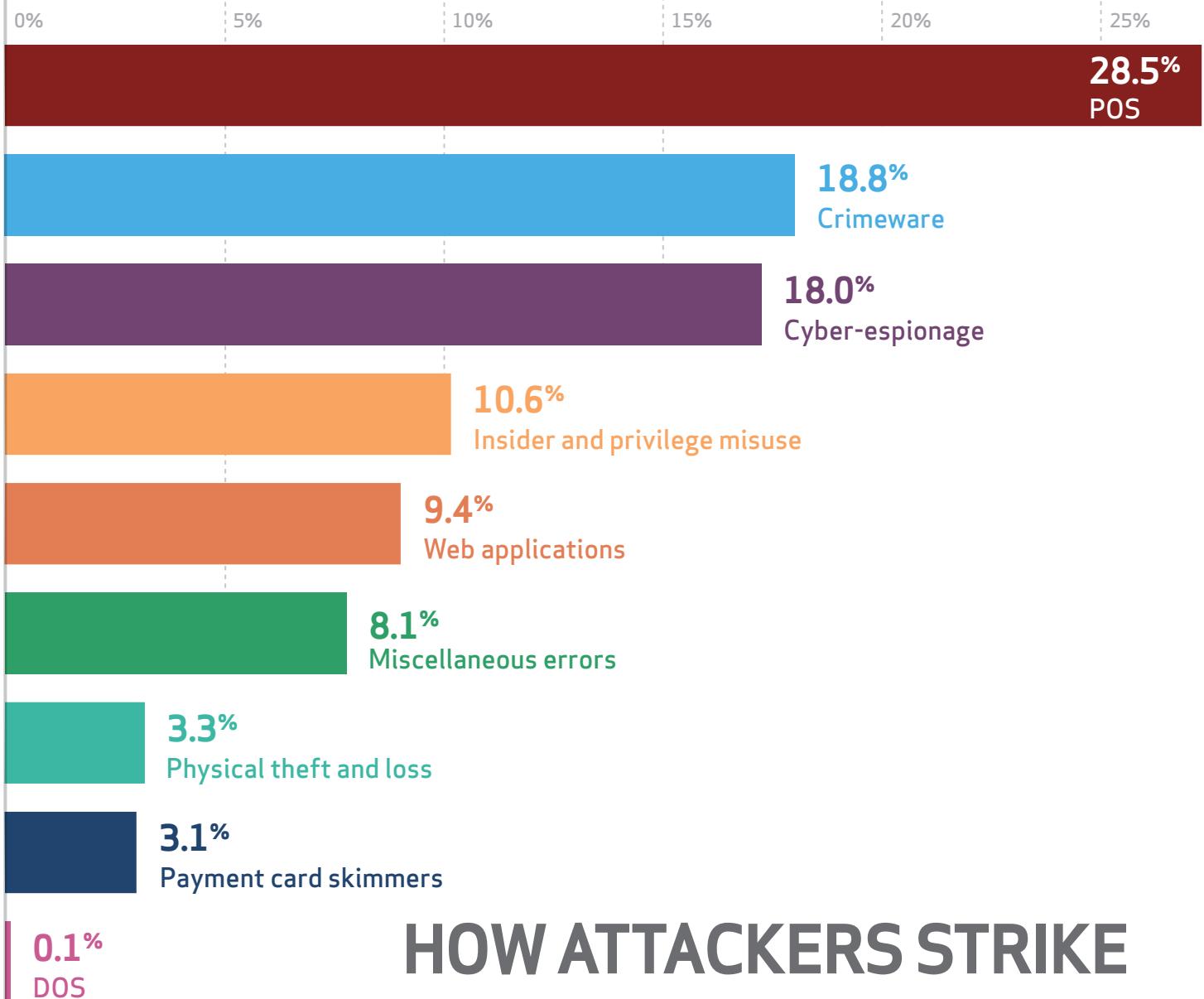


FIGURE 4
FREQUENCY OF INCIDENT
CLASSIFICATION PATTERNS



These nine patterns cover the vast majority of incidents that we've seen.

HOW ATTACKERS STRIKE

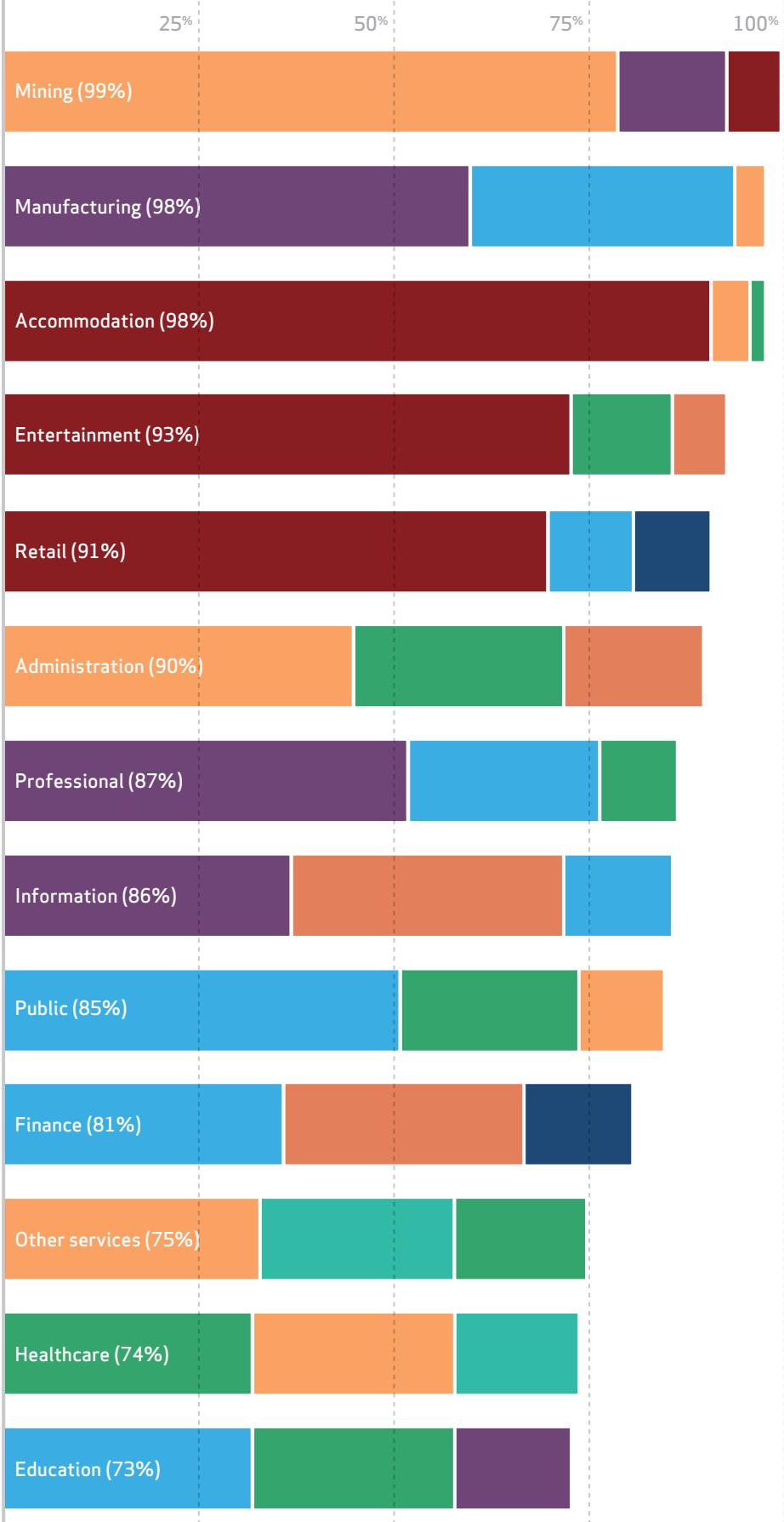
Last year we identified nine incident patterns that covered most of the security incidents that you're likely to face. These patterns cover 96% of the breaches in this year's dataset. And the majority of the threats you face are likely to fall into just three of these patterns.

The threats facing your data are becoming ever more complex and diverse. But by using statistical methods to identify clusters of similar incidents and breaches, we have developed a framework that will help you identify the biggest threats and prioritize your security investments.

Looking at all incidents, including those where there wasn't a confirmed loss of data, the common denominator across the top

three patterns is people — be it sending an email to the wrong person, failing to shred confidential information, or taking advantage of their position to harvest confidential data.

Looking at just confirmed data breaches (see Figure 4 above) provides an insight into where companies have the biggest gaps in their existing defenses: point-of-sale (POS) incidents, crimeware, and cyber-espionage.



THE TOP THREE THREATS IN YOUR INDUSTRY

Of course, each industry has its own threat profile. Understanding the main threats facing your industry enables you to make better-informed decisions about how to build your defenses.

And the good news is that, in most industries, more than three-quarters of incidents are covered by just three of the nine incident patterns (see Figure 5 left).

On average, 83% of incidents in each industry were covered by just three patterns.

You can also learn where best to focus your efforts by looking across sectors at other organizations with similar operating models. In the 2015 DBIR, we have delved deeper into our industry profiling to identify similarities in the threat profiles of subsectors from different industries.

- Point-of-sale intrusions
- Web application attacks
- Insider and privilege misuse
- Physical theft and loss
- Miscellaneous errors
- Crimeware
- Payment card skimmers
- Denial of service attacks
- Cyber-espionage

FIGURE 5 DATA DISCLOSURE, TOP 3 PATTERNS PER INDUSTRY

THE NINE PATTERNS

The nine incident classification patterns that we identified last year make it easier to understand the threat landscape, enabling you to focus your strategy, and prioritize your security investments more effectively.

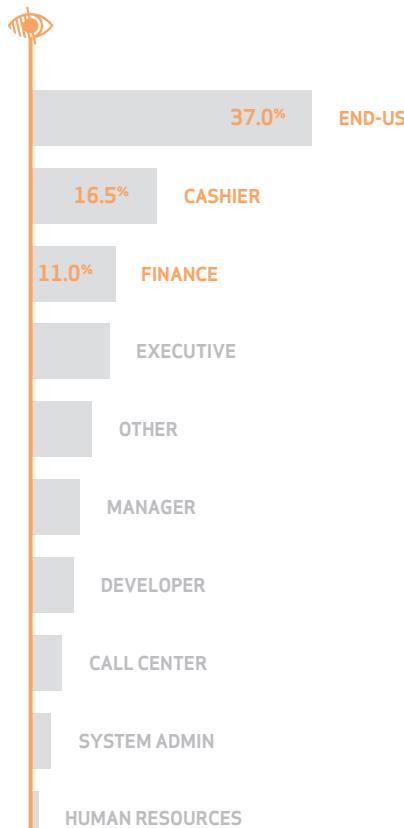


FIGURE 6
PERPETRATORS OF INSIDER MISUSE

Point-of-sale intrusions

When attackers compromise the computers and servers that run POS applications, with the intention of capturing payment data.

Most affected industries: Accommodation, Entertainment, and Retail

Smaller breaches often involve attackers simply guessing passwords or using brute force. Larger breaches may involve the breach of a secondary system to provide access to the POS system. In 2014, there were several instances where vendors of POS services were the sources of compromise. There was a shift from a reliance on default credentials to the use of stolen login details, captured through direct social engineering of employees.

What can we do? PCI DSS compliance provides a solid baseline for securing POS systems. Our 2015 PCI Compliance Report found that the areas where companies most often failed were vulnerability scanning and testing.

Crimeware

This is a broad category, covering any use of malware to compromise systems. It is typically opportunistic and motivated by financial gain.

Most affected industries: Public, Information, and Retail

This year there were hundreds of incidents that included phishing in the event chain. And in several cases trade secrets were compromised, showing that even basic malware can put your corporate data at risk.

What can we do? Patch anti-virus and browsers to block attacks and use two-factor authentication to limit any damage. And try to uncover what any malicious programs you detect were trying to achieve — this may inform where you need to prioritize your efforts.

Cyber-espionage

When state-affiliated actors breach an organization, often via targeted phishing attacks, and after intellectual property.

Most affected industries: Manufacturing, Public, and Professional

This year, there were more data breaches involving cyber-espionage than insider misuse or web app attacks. Cyber-espionage typically involves a phishing campaign, which is then used to deliver sophisticated malware.

What can we do? Patch promptly and keep your anti-virus software up-to-date. Log system, network and application activity to give you a foundation for incident response and to inform countermeasures.

Insider and privilege misuse

This mainly involves misuse by insiders, but outsiders (due to collusion) and partners (because they are granted privileges) show up as well.

Most affected industries: Public, Healthcare, and Finance

Potential culprits come from every level of the business, from the front line to the boardroom, although this year most breaches involved the end user (see Figure 6). 40% of incidents were motivated by financial gain; but employees using unapproved workarounds also caused damage.

What can we do? The first step is to know what data you have, where it is, and who has access to it. Then identify areas where you need additional auditing and fraud-detection processes. Examining devices after employees have left your company can identify any weaknesses in your defenses that you need to shore up.

Web app attacks

The use of stolen credentials or exploit vulnerabilities in web applications — such as content management systems (CMS) or e-commerce platforms.

Most affected industries: Information, Finance, and Public

Nearly all the web app attacks in 2014 were opportunistic and aimed at easy marks. Most attacks made use of stolen credentials (see Figure 7), usually harvested from customers' devices.

What can we do? Review load balancer, web application, and database transaction logs to help identify malicious activity. Use two-factor authentication and lock out accounts after repeated failed login attempts.

Miscellaneous errors

Any mistake that compromises security.

Most affected industries: Public, Information, and Healthcare

As in previous years, employees were the prime actors in most incidents. There are three main, traditional categories of error incidents: sending sensitive information to unintended recipients (30% of incidents), publishing non-public data to public web servers (17%), and disposing of personal and medical data insecurely (12%).

What can we do? To protect your data, consider implementing data loss prevention (DLP) software that blocks users from sending out sensitive information. And re-educate your employees about data security and how to dispose of sensitive material.

Physical theft and loss

The loss or theft of laptops, USB drives, printed papers and other information assets, mostly from offices and vehicles.

Most affected industries: Public, Healthcare, and Finance

Almost all theft in 2014 was opportunistic, with 55% of incidents occurring within the work area and 22% from vehicles.

What can we do? 15% of incidents in this category take days to discover. Encrypt your devices to protect the data they store and run regular backups to prevent the loss of valuable data and reduce downtime.

Payment card skimmers

The physical installation of a “skimmer” on an ATM, gas pump, or POS terminal, to read your card data as you pay.

Most affected industries: Finance and Retail

Attackers are now using thin and translucent card skimmers that fit inside the card reader slot itself.

What can we do? Monitor your pay terminals and train employees to spot skimmers and suspicious behavior.

Denial of service attacks

Use of “botnets” to overwhelm an organization with malicious traffic, bringing normal business operations to a halt.

Most affected industries: Public, Retail, and Finance

The number of distributed DoS attacks doubled in 2014. Increasingly, attackers are using the infrastructure of the internet itself to amplify their attacks.

What can we do? Know where your services are and how they're configured. Block access to known botnet servers and patch your systems. And conduct regular drills so that you can plan your defenses. You should also consider adding technology to restore services should they be compromised.

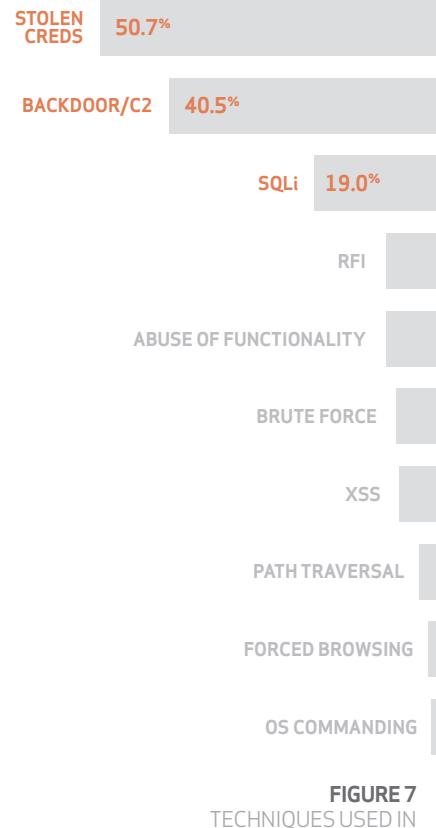


FIGURE 7
TECHNIQUES USED IN
WEB APP ATTACKS

RISKS ON THE HORIZON

In this year's DBIR we also look at some of the new potential threats that are worrying CEOs and CIOs alike. In particular, we look at the risks posed by the increased use of smartphones and tablets, and the rapid transformation of the Internet of Things from concept to reality.

0.03%

Of the tens of millions of smartphones and tablets using the Verizon network, we only see about 100 devices compromised by high-impact malware each week — that equates to less than 0.03% each year.

5bn

We predict that by 2020 there will be five billion enterprise IoT devices, and many billions more consumer ones.

Source: [Verizon State of the Market: The Internet of Things 2015](#)

The threat to mobile

Organizations are increasingly relying on mobile technology and there's a widespread concern that smartphones and tablets, especially those not controlled by the organization, could be the next opportunity for hackers. To address this concern, we've conducted our first analysis of mobile malware and related threats.

We found that Android is the most vulnerable platform — most of the suspicious activity logged from iOS devices was actually failed Android exploits. The malicious activity recorded on Android devices was centered on malware, most of which took the form of adware and other resource-wasting infections.

How big is the problem on Android? Data from Verizon Wireless showed that around 100 smartphones are compromised by high-impact malware each week, out of tens of millions of devices on the Verizon network.

We recommend that you prioritize your resources on the known methods that are being used to compromise your networks, and which are highlighted by our nine incident patterns. In terms of mobile security, seek to achieve visibility and control over how your devices are being used. This means you'll be aware of any suspicious activity and able to react quickly as the threat landscape changes.

The internet of insecure things

Not all of machine-to-machine (M2M) devices will be internet-visible or send sensitive information, but the IoT will is becoming a growing part of the IT landscape. So as you roll out new intelligent device initiatives, security should be high on your list of priorities.

There were few security incidents and little data disclosure involving M2M devices (like connected cars and smart cities) made public in 2014, but that's no cause for complacency. There have been reports of incidents involving connected devices being used as an entry point to compromise other systems and co-opting IoT devices into botnets for denial of service attacks.

So as you're thinking about IoT initiatives, we recommend that you perform threat-modeling exercises to identify your most likely adversaries and their motives, and what aspects of your M2M services are most vulnerable.

To ensure data is secure within your IoT application, you should:

- Only gather data you really need.
- Have robust consent and access controls.
- Transfer data in an encrypted and anonymized form.
- Separate data, except where you intend to perform trend analysis.

CONCLUSION: IT'S TIME TO ACT



The longer it takes you to discover a breach, the more time attackers have to cause damage. But 56% of the time it takes organizations hours or more to discover an attack — in 25% of cases it takes days or longer. And this “detection deficit” is growing.

In 60% of cases, attackers are able to compromise an organization within minutes.

When we took a closer look at the common causes of breaches, we found that nearly 25% could have been prevented by using multi-factor authentication and patching internet-accessible web services. In total, 40% of the missing controls that we identified fitted into Cyber Security’s Critical Security Controls “click win” category.

The 2015 DBIR is packed with detailed information and recommendations. But seven common themes are clear:

- **Be vigilant.** Organizations often only find out about security breaches when they get a call from the police or a customer. Log files and change management systems can give you early warning.
- **Make people your first line of defense.** Teach your staff about the importance of security, how to spot the signs of an attack, and what to do if they spot something suspicious.
- **Only keep data on a “need to know basis”.** Limit access to the systems staff need to do their jobs. And make sure that you have processes in place to revoke access when people change role or leave.
- **Patch promptly.** You could guard against many attacks just by ensuring that your IT environment is well-configured and anti-virus software is up to date.
- **Encrypt sensitive data.** It won’t stop sensitive data being stolen, but it will make it much harder for a criminal to do anything with it.
- **Use two-factor authentication.** This won’t reduce the risk of passwords being stolen, but it can limit the damage that can be done with lost or stolen credentials.
- **Don’t forget physical security.** Not all data thefts happen online. Criminals will tamper with computers or payment terminals, or steal boxes of printouts.

The Verizon Data Breach Investigations Report helps you understand the threats to your organization and improve your defenses against them. To find out more, download the full report: verizonenterprise.com/DBIR/2015.



FIGURE 8 INCIDENT TIMELINE

ABOUT THE COVER

The "universe" of dots on the cover represents 4,596 incidents from the DBIR dataset, including all confirmed data breaches over the past three years and a sample of 400 Denial of Service attacks from last year. We calculated the distance between dots using a multi-dimensional scaling technique (with the Manhattan distance algorithm) with 65 VERIS fields for each incident. This required over 6 million comparisons, and the resulting distances were projected on a two-dimensional plane. The closer the dots, the more similar the incidents, meaning they share many VERIS characteristics like threat actors, actions, assets, etc. The colors represent the nine incident classification patterns discussed throughout this report (see the Table of Contents for a section detailing how these patterns were derived). Patterns in close proximity (e.g., Misuse and Error) share many VERIS characteristics, while those that are far apart (e.g., Espionage and POS Intrusions) have little in common. The tightness or looseness of dots within each pattern shows the amount of variation among incidents in that pattern. The sub-pattern clusters (overlaid points and lines) were created using 10 years of incident data (over 100,000 incidents). We generated a forcedirected network graph from the frequency of VERIS fields and the relationships between them for each individual cluster.