Executive Summary

verizon

2013 DATA BREACH INVESTIGATIONS REPORT

A global study conducted by the Verizon RISK Team with cooperation from:

AFP Australian Federal Police

CERT | Software Engineering Institute Carnegie Mellon

Consortium for Cybersecurity Action

CyberSecurity Malaysia An agency under MOSTI

Deloitte.

EC3 Europol

ES ISAC Electricity Sector Information Sharing Analysis Center

Danish Defence Intelligence Service

FE

G-C Partners

Guardia Civil

Homeland Security

IRISS Irish Reporting and Information Security Service

POLITI

POLITIE

ThreatSim™

47,000+ SECURITY INCIDENTS ANALYZED.

621 CONFIRMED DATA BREACHES STUDIED.

19 INTERNATIONAL CONTRIBUTORS.

6TH CONSECUTIVE YEAR.

THERE'S ONLY ONE DBIR.

Verizon's 2013 Data Breach Investigations Report (DBIR) provides truly global insights into the nature of data breaches that can help organizations of all sizes to better understand the threat and take the necessary steps to protect themselves. The breadth and depth of data represented in this year's DBIR is unprecedented. It combines the efforts of 19 global organizations: law enforcement agencies, national incident-reporting entities, research institutions, and a number of private security firms — all working to study and combat data breaches.

Over the years the number of contributors has grown. Since we started publishing the DBIR in 2008, our partners have contributed data information on more than 2,500 confirmed data breaches — totaling more than a billion compromised records.

How can we turn all that raw data into information that you can use? The answer is VERIS, the Vocabulary for Event Recording and Incident Sharing. VERIS is a common, structured and repeatable language that describes *who did what, to whom, with what result*. By classifying all the information regarding the submitted breaches into this standardized format we can extract meaningful insight from what is an incredibly diverse dataset. You can find out more about VERIS at veriscommunity.net.

EXECUTIVE SUMMARY

2013 DATA BREACH INVESTIGATIONS REPORT

Will your organization, or one you work with, suffer a security breach this year? Nobody's immune, no target is too small, or too large. The methods used by hackers to gain access to data are numerous, wide-reaching and ever-growing. This isn't a threat you can afford to ignore.

All kinds of organizations — from government agencies to iconic consumer brands, internet startups to trusted financial institutions — have reported major data breaches in the last year. Many of the stories that hit the headlines are from the US, but this year's Data Breach Investigations Report (DBIR) profiles data breaches from 27 countries. This is not a localized problem, or one that you can afford to ignore. Forty-six US states already have public disclosure laws, and governments around the world, including the European Union, are actively discussing introducing mandatory reporting requirements of their own.

Disclosure laws mean that you can't keep quiet about a breach while you deal with the fallout. As well as trying to avoid being hacked in the first place, organizations need to be able to spot compromises quickly and minimize the amount of data lost.

Keeping on top of the threat landscape is a constant challenge. The best way to effectively prepare yourself is with hard data and expert analysis. The DBIR analyzes data from 19 organizations — covering more than 47,000 reported security incidents and 621 confirmed data breaches from the past year. It gives unparalleled insight into the attackers and their methods, enabling you to better protect yourself.

Verizon has been producing the Data Breach Investigations Report since 2008. This year its analysis covers more than 47,000 security incidents. Its scale is unparalleled.

This executive summary examines three commonly held assumptions about data security, and casts new light on the real risks based on the data that we've gathered. We'll look at the threat of espionage attacks on organizations of all sizes, how attacks are conducted, and your most effective defense against them. It will help you to make more informed data security decisions and reduce your exposure to financial loss and reputational damage.

69% of breaches were spotted by an external party — 9% were spotted by customers.

Social tactics — using email, phone calls and social networks to gain information on individuals — are often ignored, but contributed to 29% of attacks.

76% of network intrusions exploited weak or stolen credentials. Strict policies are required to reduce this easily preventable risk.

ESPIONAGE ATTACKS WON'T AFFECT ME

SURELY SPIES AREN'T INTERESTED IN COMPANIES LIKE MINE, ARE THEY?

Our 2013 findings suggest that there's a lot of complacency among organizations about the risk of espionage attacks. The assumption is that these attacks only target government, military and high-profile organizations, but our data shows that this increasingly isn't true. Don't underestimate the likelihood that your organization will be a target.

75% of attacks are opportunistic — not targeted at a specific individual or company — and the vast majority of those are financially motivated.

19% of all attacks analyzed in this year's report were perpetrated by state-affiliated actors — in other words, a form of espionage.

WHO ARE THE ATTACKERS?

Three key groups of actors commit cyber attacks. Each has different motivations and tactics, but the net effect of their actions is disruption, financial loss and damage to reputations. By understanding their characteristics you can be better prepared and reduce your risk.

ACTIVISTS

Activists still use very basic methods, but recent years have seen some notable and widely publicized successes. They are opportunistic, but have numbers on their side. Their aim is to maximize disruption and embarrassment to their victims.

CRIMINALS

Motivated by financial gain, criminals are more sophisticated and calculated in how they select targets. They often use more complex hacking techniques than activists. Once they've gained access, they take any data that might have financial value.

SPIES

Often state-sponsored, this group uses the most sophisticated tools to commit the most targeted attacks. They know what they want — be that intellectual property, financial data or insider information — and are relentless about getting it.

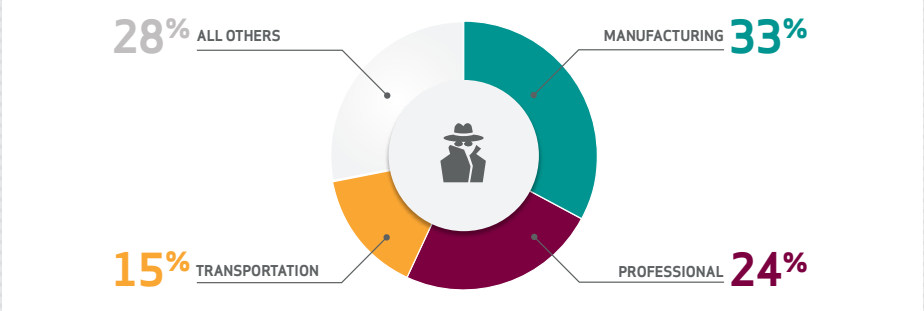
WHERE ARE THEY FROM?

The majority of financially motivated incidents we looked at originated in the US or Eastern Europe — particularly Romania, Bulgaria and the Russian Federation. Espionage cases were predominately attributable to East Asia. But the attacks that we studied happened to companies all around the world. Geographic borders are no protection against cyber attacks.

WHAT ARE THEIR MOTIVES?

In most industries, you're still much more likely to suffer an attack motivated by financial gain or revenge than espionage. Even in the industries most likely to be targeted (Figure 1), the likelihood of an espionage attack is still relatively low.

Figure 1: Espionage attacks by industry



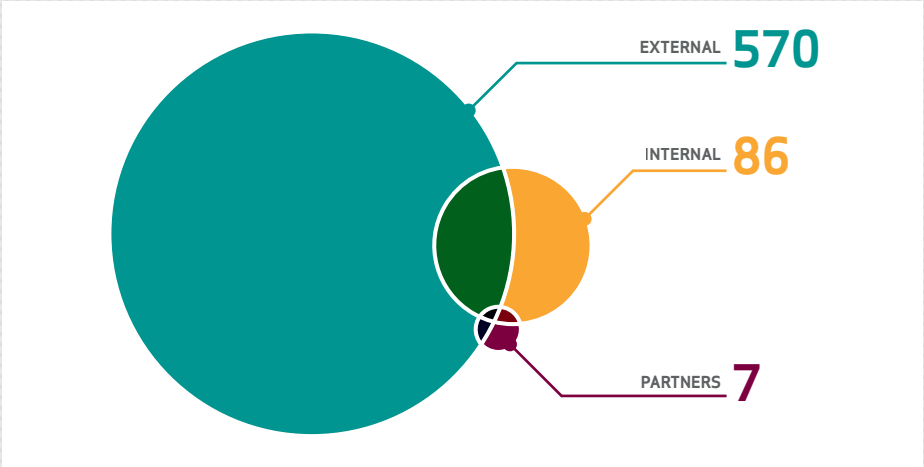
Nearly three-quarters of espionage attacks were targeted at the manufacturing, professional services and transportation industries.

But it's not just direct espionage attacks that you need to worry about. What happens if your partners or suppliers get hacked? The knock-on effect within your supply chain could be just as damaging as a direct attack. Worse still, you could be a route to an attack on one of your customers. Who would want to explain that?

WHO ELSE IS INVOLVED?

Contrary to popular belief, 86% of attacks do not involve employees or other insiders at all (Figure 2). Of the 14% of attacks that do, it's often lax internal practices that make gaining access easier than you would expect.

Figure 2: The point of origin for data breaches



534 (86%) of the breaches that we analyzed had no internal element.

Over half of the insiders committing sabotage were former employees taking advantage of old accounts or backdoors that weren't disabled.*

Over 70% of IP theft cases committed by internal people took place within 30 days of them announcing their resignation.*

* Carnegie Mellon University, http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm

IT'S BEST TO STICK WITH WHAT YOU KNOW

AS LONG AS WE LOCK DOWN THE NETWORK WE'LL BE SAFE, WON'T WE?

Many leading newspapers and journals, online and print, are full of stories about the dangers of the latest technologies. So it's little wonder that many CxOs rate cloud computing as their biggest security concern. But in the six years we've been publishing the DBIR, our data has been dominated by well-known techniques, used against the same sort of assets, again and again. This year is no exception.

MOST VULNERABLE ASSETS

1.	ATMs	30%
2.	Desktops	25%
3.	File servers	22%
4.	Laptops	22%
...		
12.	Web apps	10%

These figures add up to over 100% because sometimes more than one asset is involved in a breach.

WHAT ARE THE BIGGEST THREATS?

Very few of the breaches that we see each year surprise us. It's rare that we see something completely new, it's usually just variations on familiar themes. Well-established threats shouldn't be ignored — many are increasingly prevalent and present an ongoing danger.

It's still traditional assets (laptops, desktops and servers) that are most at risk — not the new web applications that you might be spending your time worrying about. Unapproved hardware (such as handheld card skimmers and personal storage devices) accounts for 41% of the cases of misuse in the report.

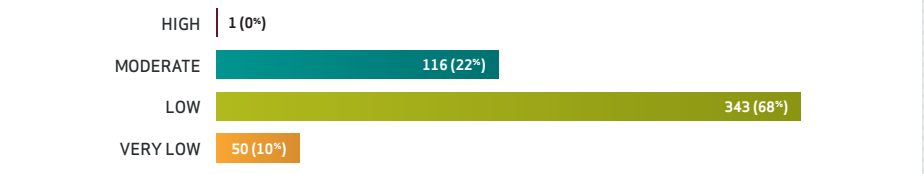
THE DIFFICULTY RATING OF ATTACKS

- **Very low:** the average person could have done it.
- **Low:** basic methods, little or no customization or resources required.
- **Moderate:** some skilled techniques and customization required.
- **High:** advanced skills, significant customizations, and/or extensive resources required.

While the sophistication of attacks is growing, most breaches could still be easily prevented.

And while perpetrators are upping the ante — trying new techniques and leveraging far greater resources — less than 1% of the breaches in this year's study used tactics rated as 'high' on the VERIS difficulty scale for initial compromise. In fact, 78% of the techniques we saw were in the 'low' or 'very low' categories (Figure 3). The barriers to entry for becoming a hacker are pretty low.

Figure 3: Difficulty of tactics used in initial compromise

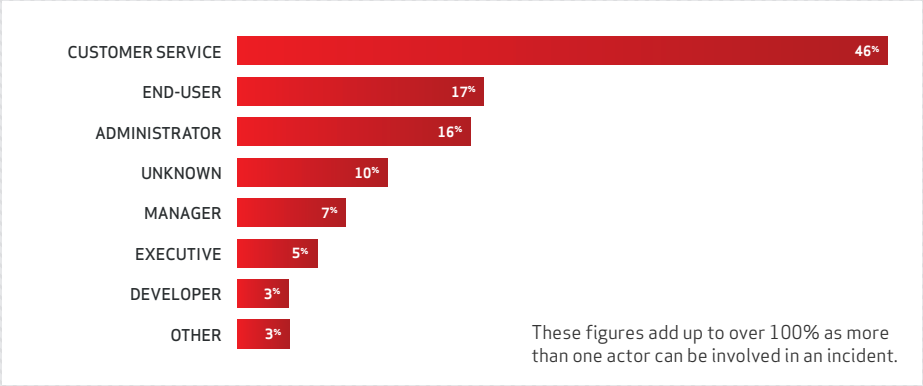


The simplicity of attacks doesn't take anything away from their effectiveness or impact. Even well-known techniques can be used to devastating effect.

WHAT SHOULD I WORRY ABOUT?

It's not just elaborate actions that have serious implications. While most breaches are deliberate, many involve an unintentional element. Taking information home, copying data onto a USB drive, attaching the wrong file to an email or sending it to the wrong person, or leaving a laptop in a cab can all lead to a data breach.

Figure 4: Breakdown of the actors involved in internal data breaches



It wasn't IT-savvy developers and administrators that were responsible for most data breaches, but customer service staff (like cashiers and call center employees) and end users. Administrators came third, but in 60% of the cases, their involvement was accidental.

From our analysis it's clear that techniques targeted at users — like malware, phishing and misuse of credentials — are major vulnerabilities. In particular, phishing techniques have become much more sophisticated, often targeting specific individuals (spear phishing) and using tactics that are harder for IT to control. For example, now that people are suspicious of email, phishers are using phone calls and social networking.

Finally, it's tempting to think that data is most at risk when it's being transmitted from one location to another. For the cases where the Verizon Investigative Response team was asked to investigate, we also tracked the state that the data was in when it was compromised. Not one breach in this sample happened to data that was 'in transit'. In fact, two-thirds of breaches involved data 'at rest' (in databases and on file servers), and the rest was being processed when compromised. Does the balance of your security efforts reflect that?

If you want to see how widely available hacking tools have become, do a web search for 'password cracker'. And in today's hyperconnected world it's highly likely that more sophisticated tools and techniques — like those used in espionage attacks — will quickly spread too.

95% of all state-affiliated espionage attacks relied on phishing in some way — even the most targeted and malicious attacks often rely on relatively simple techniques.

'Unapproved' hardware accounts for 41% of the cases of misuse in this year's study.

Not a single case where the Verizon Investigative Response team was called in — and so we could track the state of the data — involved data in transit.

IT'S OBVIOUS WHEN YOU'VE BEEN HACKED

IT'S EASY TO SPOT WHEN SYSTEMS HAVE BEEN BREACHED, ISN'T IT?

You probably have a detailed security policy and have spent a lot of money on security audits, hardware and specialist advice. So it's tempting to think that alarm bells must go off when a data breach happens. Sadly, they don't.

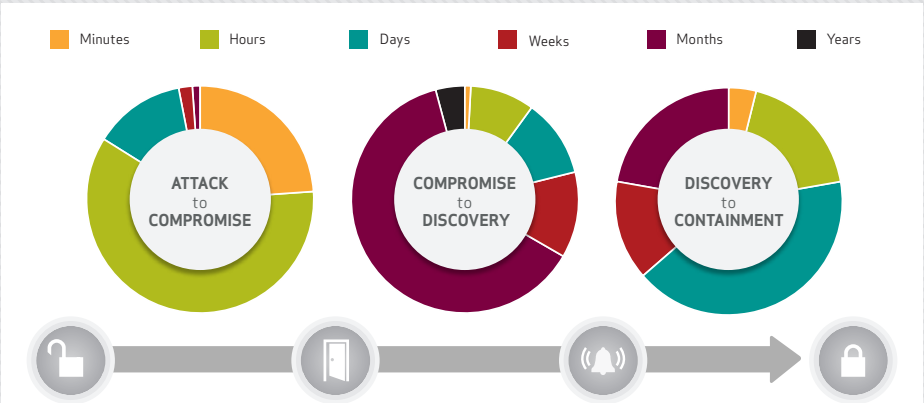
HOW LONG DOES IT TAKE TO SPOT A BREACH?

No matter how strong your defenses are, it would be foolish not to be prepared in case an attacker gets through. Organizations should be able to spot breaches and shut them down quickly, but our figures show that most can't.

66% of the breaches in our 2013 report took months or even years to discover (62% months, 4% years).

The problem is getting worse. In the 2012 DBIR, just 56% of breaches took a month or more to be discovered.

Figure 5: Timescales of data breaches



- In 84% of cases, the initial compromise took hours — or even less.
- In 66% of cases, the breach wasn't discovered for months — or even years.
- In 22% of cases, it took months to contain the breach.

It's not really surprising that many breaches happen quickly — perpetrators driven by financial gain will often quickly move on if not successful.

What's alarming is how long breaches took to spot, and how long they took to fix. And while sensitive data remains exposed, losses grow and reputations suffer further damage.

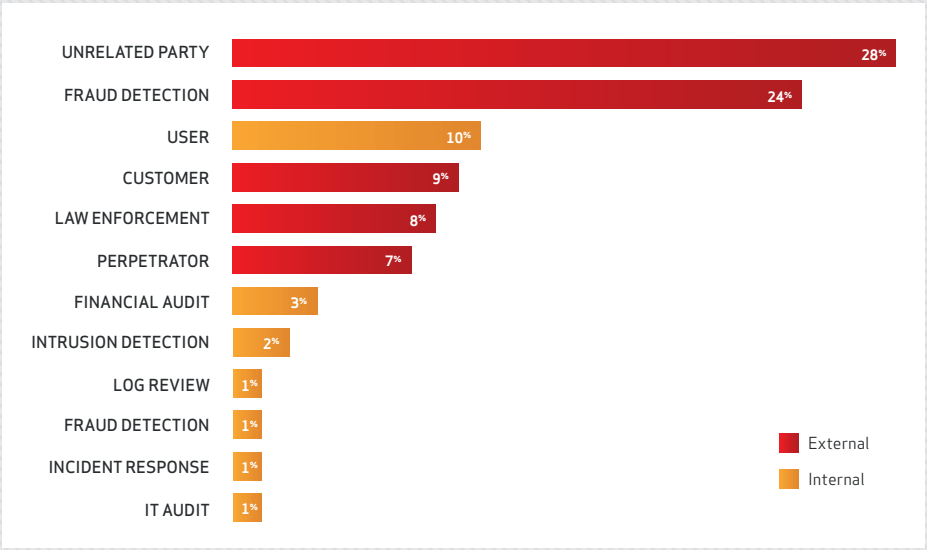
Unfortunately, this isn't a surprise. We've seen similar results in each year's DBIR.

WHO SPOTS DATA BREACHES?

Breaches were identified by a wide variety of parties — a worrying 9% of breaches were found by customers (Figure 6). Over half of the breaches identified internally were spotted by end users — not the IT team as you might have expected.

Focusing on improving processes and giving staff better awareness training could reap huge rewards, cutting the time taken to spot breaches and even preventing many from happening in the first place.

Figure 6: Who identifies data breaches



Many organizations devote a disproportionate amount of time and money to detection methods that fall below the 1% mark.

69% of breaches were spotted by an external party.

Attacks are inevitable. Companies should devote more time and effort to detection and remediation; preventing attacks becoming breaches, and breaches becoming financial and reputational disasters.

WEAKEST LINK OR GREATEST ASSET?

As we've discussed, many attacks target people. The 'carbon layer' can be a weak point, but your staff can also be your greatest asset. If you train them how to spot breaches and avoid social engineering approaches, they can be your first line of defense. The wider IT team should also be given awareness training — for example, to consider that complaints about system performance from users might be early warning signs of a breach.

9% of breaches were spotted by customers.

RECOMMENDATIONS

This summary gives just a taste of the depth of information in the full Verizon 2013 Data Breach Investigations Report. The information it offers will help you to understand the specific threats to your company — based on what you do, where you operate and how big you are — and be better prepared to tackle them effectively.

Don't buy into the idea that there's a one-size-fits-all solution to protecting your company's assets and reputation.

There's no silver bullet to preventing breaches, not even in the DBIR. Spotting and preventing data security incidents is an unending task, and one that should not be the sole responsibility of the IT department or the chief information security officer. Ensuring data security should be a company-wide effort all the way up to the boardroom. The information in the DBIR will help guide your efforts.

We'll leave you with eight key recommendations:

- Eliminate unnecessary data; keep tabs on what's left.
- Perform regular checks to ensure that essential controls are met.
- Collect, analyze and share incident data to create a rich information source that can drive security program effectiveness.
- Collect, analyze and share tactical threat intelligence, especially indicators of compromise (IOCs), that can greatly assist defense and detection.
- Without de-emphasizing prevention, focus on better and faster detection through a blend of people, processes, and technology.
- Regularly measure things like "number of compromised systems" and "mean time to detection", and use these numbers to drive better practices.
- Evaluate the threat landscape to prioritize a treatment strategy. Don't buy into a "one-size-fits-all" approach to security.
- Don't underestimate the tenacity of your adversaries, especially espionage-driven attackers, or the power of the intelligence and tools at your disposal.

VERIZON 2013 DATA BREACH INVESTIGATIONS REPORT

Download the full DBIR to read all our findings. It's the richest and most detailed source of data security trends, insights and facts there is. It will help you to target your efforts and manage data security initiatives in your organization more effectively.

verizonenterprise.com/DBIR/2013

Questions? Comments? Brilliant ideas?

We want to hear them. Drop us a line at dbir@verizon.com, find us on LinkedIn or Facebook, or Tweet with the hashtag #dbir.

In today's rapidly transforming environment, we design, build, and operate the networks, information systems, and mobile technologies that help businesses and governments around the globe expand reach, increase productivity, improve agility, and maintain longevity.

Our solutions across Connected Machines, Dynamic Cloud, Intelligent Networking and Mobile Workforce are designed to help enterprises pursue new possibilities and create entirely new revenue streams — more efficiently than ever.

Powered by investments in security, data centers, 4G LTE, cloud computing, and our immense global IP network, our portfolio of solutions effortlessly meets the demands and challenges shaping technology and business today.

We believe that businesses and individuals empowered by technology can change the world. We create solutions with that belief in mind; we perpetually challenge ourselves to enable, advance, and pave the way for new possibilities across a variety of industries.

ES15581 (Letter) 4/13