

## The Cybersecurity Playbook

By Tim Young

### We know. It's a big scary world.

According to PricewaterhouseCoopers' [Global State of Information Security Survey 2016](#), 38% more security incidents were detected in 2015 than in 2014. The theft of intellectual property increased 56% in that same time period, according to the report, which relies on survey responses from more than 10,000 C-suite executives, VPs, and directors of IT and security practices hailing from 127 countries.

At the same time, the survey shows that firms are taking steps to address these threats. Respondents said they boosted their information security budgets by 24% between 2014 and 2015, and report that financial losses decreased 5%. So it would seem that many firms are finding a way to stem the tide; but the seemingly endless deluge of threats requires a level of vigilance that simply wasn't required in, say, 1995 when the movie [Hackers](#) was released.

If you've watched it recently, it's a perfect storm of floppy disks, Angelina Jolie pixie cuts, and third-rate electronica. But behind all that silliness is an image of cybercrime that is downright quaint by today's standards.

Hacking is treated like some kind of magical trickery that can only be accomplished by leather-jacket-clad teenagers and the fruit hangs oh-so-low because no one seems to know how to protect their assets from these rascally wizards.

But the massive advances in both cyberthreats and cybersecurity have been a mixed blessing.

### The scope of the problem

On the negative side, the volume and severity of threats have increased. Security firm Gemalto reported in its [2015 First Half Review](#) that, in the first six months of this year, nearly 246 million records were breached in 888 separate incidents. The top 10 breach incidents



alone exposed 82% of the affected records and, in half of the breaches, it is unknown how many records were compromised.

Kaspersky Lab, meanwhile, reported that in Q2 2015 alone, their solutions detected and repelled a total of nearly 380 million malicious attacks from perpetrators located all over the globe. Almost 6 million of those were attempted malware infections designed to steal money by tapping into a user's online banking portals.

However, those numbers also demonstrate the flip-side of the current cybersecurity landscape. Many of these threats were detected and repelled. We have the tools to resist many of these exploits, and we also understand a crucial truth about cybercrime: the methods may be sophisticated, but the motives rarely are. Attackers want access without working too hard or spending too much to get it. Simple vigilance can go a long way toward repelling the bulk of attacks.

As security maven, Eugene Kaspersky [told the Boston Globe](#) recently, attacks can't be stopped, but organizations can make themselves hard targets by increasing their security to a level at which they are difficult, expensive and time-consuming to breach. Or, as he told the Globe, "You want to make the hack more expensive than the possible damage."

And a good place to start is by covering your bases on nine basic types of intrusion.

In 2014, Verizon headlined its annual Data Breach Investigations Report (DBIR) with the statistic that 92%



Not for distribution or reproduction.

of the 100,000 incidents they analyzed in the past 10 years fell into nine basic categories. (You can read that 2014 report [here](#).) When they released the 2015 report in April, they revealed that not only did that pattern hold over the last year, it actually increased to 96%. So these patterns are a great place to start.

## Top 10 Cybersecurity Threats:

### 1. Miscellaneous errors

Yep. Not scheming criminals in black hats or Bond-villain-esque autocrats hacking away in faraway data centers. The top cause of incidents in the 2015 DBIR is user error, including misdelivery of sensitive information to the wrong recipients, publishing of non-public data to public servers, and improper disposal of sensitive data.

These errors accounted for nearly 30% of incidents examined by the DBIR (though only about 8% of confirmed breaches). The good news is that while this is a difficult problem to completely eliminate—mistakes happen when human beings are involved—there are ways to minimize this problem through process enhancements. One tool that comes to mind is data masking, the location and de-identification of sensitive data that can render errors such as these less critical. I wrote more about this [a few months ago](#), but it's an interesting and growing field, with Informatica, IBM and Oracle leading the way.


### 2. Crimeware

Verizon uses this term to differentiate malware with functionality like command-and-control (C2), DOS, backdoor, keylogger and downloader from more specialized classification patterns such as cyber-espionage or point-of-sale (POS) intrusion. Crimeware is involved in 28.5% of incidents and 18.8% of confirmed breaches in the DBIR.

Vigilance with basic anti-virus programs goes a long way toward preventing this “in.” [According to Gartner](#), Symantec is still the market leader on that front, followed by Intel (including the McAfee properties), IBM (which saw 17% growth in this market in a year when the market as a whole only grew 5.3%), Trend Micro and EMC.

### 3. Insider misuse

Once again, a threat from the inside causes major issues. Whether it's a cashier looking to ring up some charges on a stolen credit card account, an end user looking to simplify access to sensitive information, or a developer trying to implement a time-saving workaround



*“You want to make the hack more expensive than the possible damage”*

without considering risk, insider misuse and abuse is a big problem.

Verizon reports that two of their partners—Winston & Strawn and Mishcon de Reya-- have had great success with remedies for insider abuse. The key is to be able to collect and collate data logs of the users' digital footprints so that the data can be analyzed and legal measures promptly pursued before further damage is done.

Solutions such as Nakina Systems' NI-GUARDIAN are handy on this front, as they get rid of shared passwords; assign privileges by role, location and time; and give a complete “flight-recorder” log of all interactions. (Nakina scored a Pipeline Innovation Award this year because of their forward-looking security and assurance solutions.) Products with some similar functionalities exist from a number of vendors, including Accurate Always, who was a runner-up for our Innovation Award for security for its Voxida CenterSecure solution that keeps tabs on and controls permissions for help center employees and contractors.

### 4. Physical theft/loss

Sometimes people steal things. Sometimes those things are laptops or other hardware containing sensitive data. Encryption helps. Data masking helps. Locked doors and guard dogs help. Not much else to say about that. But these physical thefts account for 15% of incidents recorded by the DBIR.

### 5. Web app attacks

Now we're starting to get into the rarer occurrences, as far as individual incidences go. Web app attacks account for just over 4% of the incidents studied by the DBIR. Organized crime was the most common perpetrator, and most of the victims were easy marks. Some 95% of the incidents involved pulling credentials from stolen consumer devices and using them to log into web apps. Two-factor authentication can cut down on this threat.

## 6. Denial-of-Service

Distributed denial-of-service (DDoS) attacks are still a problem. Just a few days ago (as of my writing), British service provider TalkTalk was hacked, and a [DDoS attack provided the smokescreen](#) for the serious damage.

Government web services also get jammed up by DDoS attacks with some regularity, [the most recent example](#) that comes to mind being the Thai government's website at the end of September.

This type of attack is of particular concern for Pipeline readers, as it falls on the shoulders of the CSPs. Verizon's advice in the DBIR for its fellow CSPs is not dissimilar to my advice on the physical theft item: lock your stuff up. "Secure your services (which means knowing where your services are and how they're configured)," the report authors recommend. "Block access to known botnet C2 servers 50 and patch your systems to help stop malware from turning your nodes into hapless automatons of doom." They also note that anti-spoofing filters at the Internet edge can help larger providers block common amplification techniques.

## 7. Cyber-Espionage

Finally! The exciting stuff! International intrigue! I can just imagine roomfuls of hackers at the NSA or in China or North Korea slipping into all corners of the web.

Except that very few cyber-espionage attacks left behind any attacker-attribution of any kind, according to the DBIR. Plus these are rare, accounting for 0.8% of recorded incidents. What we do know is that the majority of these intrusions were on manufacturing (27.4%), public (20.2%), professional (13.3%), information (6.2%), and utility (3.9%) targets. Targets like financial services, healthcare and retail barely register (all under 1%). This tells us a little about who should be bringing in the big guns to protect against cyber-spies. According to the DBIR, the most commonly taken information in these intrusions were secrets (85.8%), followed by credentials (11.4%).

These are sophisticated attacks and difficult to guard against, but the takeaway for most of us is that these aren't attacks that are leveled at the average individual or firm. However, one good takeaway is that reliable Big Data solutions can help you better understand what, if anything, has been snagged by one of these attacks.

## 8. POS Intrusions

This one's for those retailers who were just told to not worry about espionage. Point-of-sale intrusions account for only 0.7% of incidents, but a whopping 28.5% of

*You'll notice that there's been no mention of mobile malware. That's because it isn't a big issue... yet.*

confirmed data breaches. While these were long thought of as petty crimes involving low dollar amounts, they are increasingly a genuine threat.

Passwords are often gathered from low-level employees using simple social engineering (a phone call from a phony supervisor, for instance), and it's hard to combat that sort of thing. However, everything that was true for the errors and insider misuse sections can apply here, too. Removing default passwords, implementing two-factor logins, and controlling credentials are all helpful tools for combatting POS intrusions. Also, since the actual intrusions are often preceded by crimeware that paves the way, taking a look at software can be helpful.

## 9. Payment card skimmers

This one is arguably the rarest of the bunch, accounting for 0.1% of incidents and 3.1% of confirmed breaches. Criminals have gotten better at mounting phony readers on gas pumps and on ATMs, including thin, translucent devices that mount inside of existing readers. It's the future! Chip and PIN technology, which is finally taking off in the U.S., was supposed to make these issues less of a problem; but poor implementations still create big, wide openings for ne'er-do-wells. Merchants are the front line on this one, and need to up their fraud management game and make sure that chip and PIN systems are well-implemented.

## 10. Mobile malware waiting in the wings

You'll notice that there's been no mention of mobile malware. That's because it isn't a big issue... yet. In one of the DBIR's catchier subheads, you'll see that providers have "got 99 problems and mobile malware isn't even 1% of them." (I think that line was a little smoother when Young Hov laid it down, but I could be wrong.) Out of all the millions of mobile devices, an estimated 0.03% were infected by legitimately malicious malware, according to the DBIR. Now, that rate is bound to change; but until it does, we'll let other journalists jump on the mobile malware train.

Not for distribution or reproduction.

And yes, this list doesn't cover every single possible threat, but it does hit the big ones. The disturbing trend is how many providers and other firms haven't done enough to combat the above. So while they wait on some exotic threat to cripple us, they may just have a sticky-fingered employee or a well-meaning CSR crippling their otherwise well-oiled machine.

How prepared are you?