WHITE PAPER

Lessons from Gemalto's 2018 Breach Report

Cybersecurity Trend Insights from Tripwire Experts

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Breach data from the first half of 2018 shows us where cybercrime trends are headed, with several major departures from 2017's stats. Gemalto's *H1 2018 Breach Level Index Report* analyzes the data behind 945 breach incidents—more than 4.5 million breached records. The breach data is categorized by risk score, geography, industry and more.

In this white paper, Tripwire experts interpret the report into actionable steps to help you avoid repeating the breaches that rocked the cybersecurity world in 2018. As is often the case, making sure you aren't the victim of a cyberattack largely comes down to how well you implement basic, foundational security controls like integrity monitoring, event logging and vulnerability management.

The Data Shows 133% YoY Breach Increase

Gemalto's breach index found that more than 3.5 billion records were breached in H1 of 2018—that's 291 records per second, marking 2018 as the worst year yet for worldwide data theft. According to the report, "That figure marks an increase of 72 percent over H1 2017."

The report breaks these breaches down by type. It assigns each one a risk score based on the quantity of compromised records and what was done with them once they got into the wrong hands. Here are the stats on who the bad actors were, what their motives were, and which industries they hit the hardest.

Breach Actors

Malicious Outsiders at #1

Whereas the most common source of data breaches in 2017 was accidental loss, H1 2018's primary breach actors were malicious outsiders. They were behind 56 percent of all breaches, followed by accidental loss at 34 percent, malicious insiders at 7 percent, hacktivists at 2 percent, and the remaining 1 percent falling into "unknown." Hacktivism and malicious insider breaches both saw a decrease this year.

Breach Motives

A Big Spike in Identity Theft

Sixty-five percent of breaches were identity theft, indicating an explosive 1,128 percent increase compared to last year. The sheer number of individuals who experienced identity theft in this period is something to reckon with: Companies who store customer data need to ramp up digital security, and fast. Trailing behind are breaches motivated by account access at 17 percent, financial access at 13 percent, nuisance at 4 percent, and existential data theft (intellectual property, for example), at 1 percent.

Breaches by Industry

Social Media Ranks Worst

Social media companies were responsible for the highest number of compromised records at 56 percent, thanks in part to the enormity of their user base. Behind that was government at 27 percent, with "other industries," retail, tech, industrial, education, healthcare, financial and more holding the lower breach rankings. The industry with the sharpest rise in breaches was industrial, growing an unprecedented 83,787 percent over last year.

Industrial's Hour of Reckoning Has Arrived

Outside of social media, the industrial vertical saw the highest growth rate of breaches. This is likely due to increasingly-connected IIoT equipment introduced into legacy OT environments, as well as a lack of cybersecurity expertise among ICS operators who are used to unsegmented (read: unprotected) networks. Luckily, tools that enforce compliance with regulations (e.g. NIST, NERC CIP, ISO and others) help organizations align with prescriptive policies, procedures and technologies to minimize their attack surfaces.

The Four Biggest Breaches

Gemalto ranked the breaches in their report with risk scores. Scores of 1–3 present "minimal" risk, 3–5 are "moderate," 7–9 are "severe," and 9–10 are "catastrophic." All of the top four breaches covered here fell into the catastrophic risk score.

Facebook

Identity Theft by Malicious Outsider

Facebook has been the subject of several notable data breaches, with far-reaching implications about the current state of social media data privacy. But this one was a doozy, exposing the personal data of its entire user base of more than 2 billion. When a giant like Facebook gets breached, a significant percentage of the world's population is impacted. This particular breach took place by way of Facebook's account recovery and search features, which allowed hackers to scrape personal data on an incredible scale.

» **Tripwire solution:** This could have been avoided by having an effective log management solution in place. For example, Facebook should know how many account recovery requests happen per week. If they'd been effectively monitoring their event logs, they would have noticed a sudden increase in account recovery requests alerting them to investigate.

Aadhaar

Identity Theft by Malicious Outsider

Aadhaar numbers are India's citizen ID numbers, a 12-digit string of numerals connected to each person's name, address, photo, email and phone info. Reporters at Tribune News Service found an anonymous seller advertising on global messaging app WhatsApp that later led to this breach's discovery. The ads they found offered access to Indian citizens' Aadhaar numbers to anyone who could pay 500 rupees—that's the personal data of 1.1 billion people.

» **Tripwire solution:** Government agencies can use foundational change management controls to quickly identify deviations from their systems' secure baseline state. File integrity monitoring (FIM) and security configuration management (SCM) solutions detect unauthorized changes the moment they occur. When cybercriminals breached the Indian social security system, there was certainly a new file executing a script or taking an action on a critical server. Security best practice frameworks like MITRE ATT&CK, which advanced FIM and SCM tools can be made to enforce, use real-world attack vector scenarios to harden systems.

Exactis

Identity Theft by Accidental Loss

Data-aggregation firms like Exactis are in an extra-precarious cybersecurity position because of how much (and which types) of data they store. This breach occurred when they unknowingly left 340 million records exposed on a publicly-accessible server. Within the two terabytes of exposed data contained highly-sensitive information like physical addresses and the names and genders of consumers' children.

» **Tripwire solution:** Exactis could have avoided this breach using a comprehensive vulnerability management (VM) program. Advanced VM tools allow organizations to scan from outside their networks to get an attacker's view and identify open database servers.

Under Armour

Account Access by Malicious Outsider

If you've ever used the app MyFitnessPal to track your diet and exercise you may be one of the 150 million people whose personal data was breached back in March. Under Armour's app was compromised when a cybercriminal got access to a piece of their software. Only usernames and email addresses were exposed—not payment card information—but this was still the biggest retail breach in recent memory.

» **Tripwire solution:** Similarly to Aadhaar, this breach could've been quickly nipped in the bud with a change monitoring solution flagging deviations from Under Armour's secure baseline. More specifically, this was likely a change that occurred in their active directory groups and users. The attacker could've used privilege escalation, a common attack vector for this type of breach. Monitoring the groups and users for permission changes is a fundamental part of any good change management program.

Protect Your Data with Foundational Controls

Foundational security controls would have prevented all four of these major breaches, yet cybersecurity programs often lack these core processes. Foundational controls include privilege management, VM, change control, centralized log management and incident response. While you shouldn't stop there, getting a handle on the foundational controls is where many organizations need to start.

Security controls can be considered on three tiers: foundational, fundamental and advanced. Too many companies think that by focusing on the latest, most advanced technologies, such as AI and machine learning, they can keep ahead of cyberthreats.

But in reality, very few cyberthreats are blocked by focusing only on these technologies. The vast majority of common

> "Change detection is a foundational control every security and compliance program should implement. Understanding what you have, securing it, and continuously monitoring for changes is the most effective way to mitigate cybersecurity risk."
>
> — Rod Musser, Tripwire Senior Product Manager

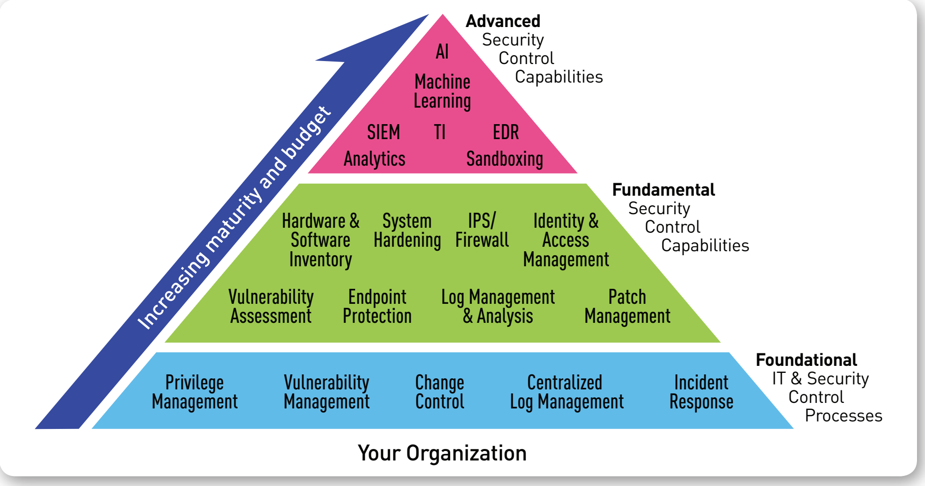

Fig. 1 Tripwire's flexible data collection works throughout your network to help ensure availability, security and resilience

threats can be prevented by focusing your investment on foundational IT and security processes.

Gemalto's report is evidence that threats are mounting, especially in terms of identity theft and malicious outsiders. Luckily, these foundational controls can mitigate the most risk in your environment and will protect you regardless of the source of the hack.

"Organizations that use Amazon Web Services S3 buckets and other cloud-based assets to store their data can't assume that they're automatically protected against a security incident. They need to remember that there's such a thing as "security in the cloud," which means they have a responsibility to protect their cloud-based data by using encryption and other security practices, managing privileged access and maintaining compliance."

— Gemalto Breach Index Report H1 2018

Tripwire Enterprise for Cloud Security

Organizations using Tripwire® Enterprise have the security benefits of foundational controls on their side from the inventors of FIM. One example pertinent to the biggest breaches of the year is S3 bucket monitoring in AWS. If an S3 bucket is accidentally (or maliciously) made public, *anyone* can access it instantly. Tripwire Enterprise, which covers on-premises, cloud-native, and hybrid systems, monitors S3 buckets for permission changes to prevent this from occurring.

Request A Demo

Let us take you through a demo and answer any questions you have. Understand how Tripwire's suite of security and vulnerability management products and services can be customized to specific IT security and compliance needs.

Visit tripwire.com/contact/request-demo to schedule your demo today.

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at** tripwire.com

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » **Watch us at** youtube.com/TripwireInc