ACHIEVING DATA-CENTRIC SECURITY

HOW TO FEND OFF BREACHES BY BEING BRILLIANT AT THE BASICS

Accenture Security

DATA BREACHES HAPPEN WHEN ORGANIZATIONS FAIL AT FUNDAMENTAL DATA PROTECTION PRACTICES.

A fresh look at those practices can make your organization and your high-value assets more secure.

INTRODUCTION

Consider for a moment some of the most significant data breaches of the recent past:

- More than 140 million customer records exfiltrated from a leading credit reporting agency, exposing highly valuable personally identifiable data, such as Social Security numbers, dates of birth and driver's license information.
- Half a billion user accounts compromised at a leading Internet service provider, revealing names, e-mail addresses, telephone numbers, dates of birth, password information and more.
- 80 million patient and employee records breached at a health insurer, potentially exposing names, dates of birth, Social Security numbers, e-mail addresses, employment information and income data.
- More than 50 million credit card accounts compromised at one leading retailer, and more than 40 million at another.

The list goes on. But when you take a step back to assess what these breaches share in common, you reach an inescapable conclusion: the numbers would be on a less staggering scale if the organizations involved had effectively practiced the basics of data-centric security.

Now, more than ever, it is critical for every organization serious about protecting its data to review and implement these data-centric security fundamentals.

WHAT SIGNIFICANT DATA BREACHES SHARE IN COMMON

Let's start with the obvious. Data breaches of the scale in the examples cited are **incredibly costly.** Estimates put financial losses from a severe event into the tens or even hundreds of millions of USD. Add on to that damage to brand and reputation, and ongoing financial and legal exposure. The pain can be immense and long lasting, to both the victimized organizations and their partners and customers.

Even in everyday breaches of more manageable scale, the financial and reputational damage takes a toll; research by the Ponemon Institute sponsored by Accenture estimates the cost of cyber crime to the average organization has increased by nearly 23 percent in the last year to US$11.7 million.

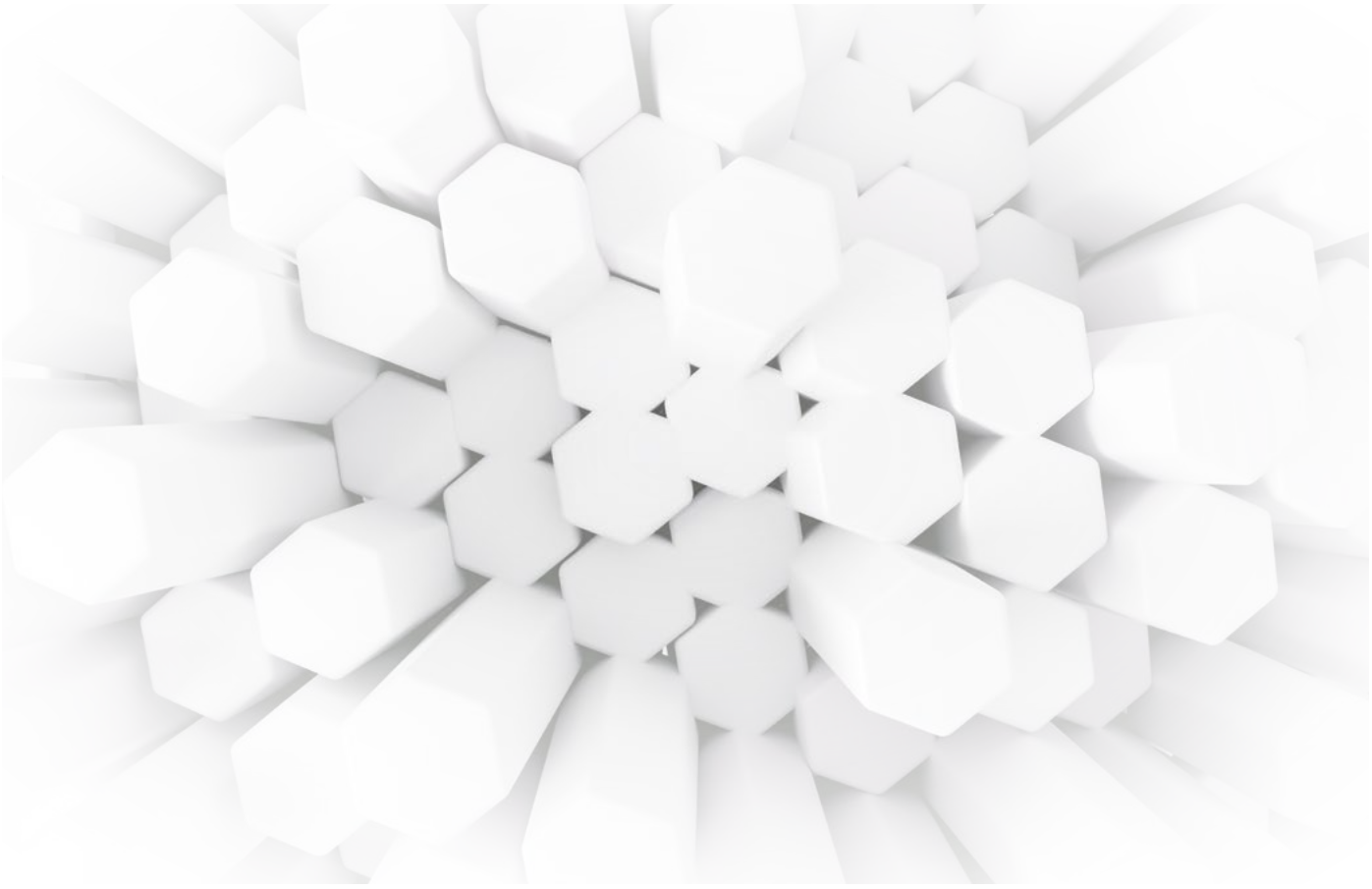
A related similarity is that organizations victimized by breaches **have not fully appreciated the value of data as the lifeblood of business.** In the intelligence community—think Central Intelligence Agency, MI6, Mossad and the like—loss of data means loss of life. Hence there is an absolutely urgent focus on protecting data to save lives. In business, losing data may also cost lives in sectors like energy, chemicals and healthcare, but it is more likely to lead to competitive disadvantage, damage to brand and reputation, and significant legal and financial consequences. Business runs and depends on the secure processing of data, and protecting data deserves a commensurate level of attention, respect and investment. In the digital era, data is value. Those who guard that value have significant advantage over those who do not.

The third characteristic shared by organizations victimized by breaches is **multiple points of failure.** The issue is not whether criminal attackers exploited a known website vulnerability the victim organization failed to patch, or instead launched a zero-day attack. The issue is that multiple

“Harden” your high-value assets.

processes and procedures had to fail for tens of millions, or hundreds of millions, of customer records to be exfiltrated, and for that exfiltration to go undetected for days, weeks or months.

All of which adds up to straightforward, prescriptive advice: Organizations need to put their data protection fundamentals in order. To fend off and minimize the impact of data breaches, they need to “harden” their data assets and be brilliant at practicing data-centric security basics.



BE BRILLIANT AT THE BASICS

IDENTIFY YOUR HIGH-VALUE ASSETS

These are your "crown jewels"—the data most critical to your operations, subject to the most stringent regulatory penalties, and most important to your trade secrets and differentiation in the market.

HARDEN YOUR HIGH-VALUE ASSETS

"Hardening" high-value assets means making it as difficult and costly as possible for adversaries to achieve their goals, and limiting the damage they can cause if they do obtain access. Some added guidelines:

- **Adopt the attacker's mind-set.** What do they want most? Design and execute your threat and vulnerability program, and overall security solution, to deny it.
- **Consider and use multiple techniques** including encryption, tokenization, micro-segmentation, privilege and digital rights management, selective redaction, and data scrambling.
- **If your high-value assets are on legacy systems, do not try to harden those assets all at once.** Instead, add additional protection and increase visibility over control points or points of access until you migrate or modernize the legacy systems. If you have legacy systems that cannot be suitably hardened, look for opportunities to restrict access and up-level your monitoring. Be laser-focused on timely detection at your weakest links.
- **Remember that with all the focus on securing data—encrypting it, keeping it in the safest of systems—if the same controls are not applied to people who have access to the data, you have simply moved the point of failure.** To fully protect your high-value assets, it is critical to keep "the people dimension" in mind.

BUILD UP YOUR DEFENSES THROUGH NETWORK ENCLAVES BOTH ON-PREMISES AND IN THE CLOUD

The perimeter is no longer the perimeter—it has become too easy for adversaries to breach. And the enterprise that the perimeter is intended to protect now extends well beyond "the four walls" to the cloud and the field and the control rooms. Consider creating enclaves—environments both on- and off-premises where you can better monitor the comings and goings of users and the behavior of applications—which limit an attacker's maneuverability. When the perimeter is breached, the enclaves remain safe. Think of a ship—if the hull is breached, hard partitions in the compartments underneath will prevent the ship from sinking. In the same way, hard-partitioned enclaves in your network prevent a breach from moving laterally through the entire enterprise.

BUILD AND EXECUTE A HUNTING PROGRAM

There was a time when organizations felt they only had to activate their incident response plans in the event of a breach. Not any longer. Today, the best approach is to adopt a continuous response model—always assume you have been breached, and use your incident response and threat hunting teams to always look for the next breach ("find them before they find you").

Enclaves in your network can prevent an adversary from moving laterally through the entire enterprise to access your sensitive data.

BE BRILLIANT AT THE BASICS

Timely patching of systems is difficult, but an essential priority.

BUILD AND USE ADVERSARY SIMULATION AND CATASTROPHE SCENARIOS

Run and test those scenarios for end-to-end effectiveness —so that you can verify and validate that you can detect an adversary, and that your people are prepared and ready.

SCAN YOUR APPLICATIONS

Scanning is important because it helps identify actual vulnerabilities—ideally as soon as they are discovered and reported—but it is only one component in an overall security framework. To optimize scanning efforts, have as complete a grasp as possible on your external assets—know what you need to scan. Know who owns the assets and who can fix vulnerabilities. Make sure your security team can validate scanning results and quickly eliminate false positives. Integrate security into the development cycle itself, so that bugs get fixed prior to scanning, more cost-effectively. Measure the resolution time for vulnerabilities and help the business prioritize remediating those which pose the greatest risk. Application scanning is not just having a tool, but having a robust end-to-end program to decrease security risk in a cost-effective manner.

PATCH YOUR SYSTEMS

It sounds easy, but it takes forethought. Organizations fail to patch their systems because they have a fluid system landscape. They do not know how many systems are active

in their inventory. If they do have an inventory, they might not know all the different versions of software on their platforms; a patch to a certain version of an operating system might break the application on top of it. A threat intelligence program can provide automatic notification when specific applications with high-value assets require a patch to avoid being exploited. The program must also reconcile anomalies, such as a patch that requires a reboot on a system prohibited from rebooting.

LIMIT, MONITOR AND SEGMENT ACCESS

Use two-factor authentication as much as possible, and use role-based access to make automated decisions about who is allowed to see what data and systems. Move toward micro-segmentation in your access control, recognizing that when sensitive data needs to be adjudicated by different people for different reasons, none may need to see the data in totality. Micro-segmentation can show each person what he or she needs to see based on his or her roles and responsibilities, while obscuring the rest. This also limits damage in the event of a breach—if any one user's credentials are compromised, only a portion of the data is exposed. To exfiltrate whole objects or larger swaths of data, the adversary's job becomes much more difficult.

MONITOR FOR ANOMALOUS AND SUSPICIOUS ACTIVITY

Monitor continuously and vigilantly not just for unauthorized access but also for undiscovered threats and suspicious user behavior.

Show each person what they need based on roles and responsibilities and obscure the rest.

BE BRILLIANT AT THE BASICS

DEVELOP BOTH STRATEGIC AND TACTICAL THREAT INTELLIGENCE

Have a sustainable threat intelligence program that collects and curates both strategic and tactical threat intelligence. Strategic threat intelligence is human intelligence coming from a variety of both closed and open sources—for example, an e-mail explaining that certain versions of Apache Struts are vulnerable to attack, and how that vulnerability is exploited. Other forms of strategic intelligence can provide insights on campaigns targeting certain industries or technologies, or geo-political trends that could change the incentives of attackers. Tactical threat intelligence includes machine indicators of compromise that feed in automatically to your systems—for example, an automatic feed from Palo Alto Networks or Qualys directly into your tooling. Stay as current as possible on both the broader threat landscape and the specific threats posed by adversaries as they relate to your organization.

BUILD A SECURITY ECOSYSTEM

No organization is an island. Supplement internal talent and skills with a diverse vendor support system. When necessary and appropriate, take advantage of the assistance that managed services organizations can deliver.

PREPARE FOR THE WORST

Transform your incident response plan into a crisis management plan that can be enacted if the worst-case scenario materializes. Make sure legal and corporate communications teams are on “stand by” and prepared to take action. Exercise the plan so that the business builds the muscle memory and identifies areas for improvement before the

next issue arises. Be ready for a catastrophic cyberattack where e-mail, voice over IP, and other communication systems used on a day-to-day basis are unavailable. For such catastrophic emergencies, consider storing critical contact information in the cloud and being prepared to use the cloud as a secondary out-of-band platform for e-mail and voice communication.

ANY ORGANIZATION INTENT ON AVOIDING SERIOUS DATA BREACHES OWES IT TO ITSELF TO REVIEW HOW WELL IT IS PUTTING THE FUNDAMENTALS OF DATA-CENTRIC SECURITY INTO PRACTICE.

Closing any gaps will help fend off breaches and minimize their impact.

Find out more about the evolving cyber security landscape and what you can do to strengthen your defenses.

CONTACT

Ryan LaSalle
Managing Director, Growth & Strategy
Accenture Security
ryan.m.lasalle@accenture.com

Justin Harvey
Managing Director, Incident Response & Threat Hunting, Accenture Security
justin.harvey@accenture.com

Rick Hemsley
Managing Director, Accenture Security
rick.hemsley@accenture.com

Gareth Russell
Managing Director, Accenture Security
gareth.russell@accenture.com

Visit us at www.accenture.com

Follow us @AccentureSecure

Connect with us

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 411,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com.**

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us **@AccentureSecure** on Twitter or visit the Accenture Security blog.