SECURITY COMPASS WHITEPAPER

What's the Real Cost of a Data Breach?

Learn about the impact of security breaches on your organization and how you can implement reasonable security measures to improve product security.

Security Compass

Brand damage from data breaches can be irreversible

The 2017 Equifax data breach exposed the personal information of over 147 million American, Canadian, and British citizens. Like many breaches, this resulted in financial penalties, including fines imposed by the U.S. Federal Trade Commission (FTC) of up to US$700 million. The financial consequences did not end with a fine, however. The market also punished Equifax, resulting in a drop in their stock price of over 30 percent and a loss of over US$5 billion in market capitalization.

Do you know how much your personal data is worth on the dark web?

Impact of the Equifax Data Breach

As one can imagine this earned the attention of Equifax's board of directors. The results were not good. Within weeks, the CEO, CIO, and CISO "retired" (effective immediately). Even worse, one executive who learned of the breach exercised and sold all his options in anticipation of the price decline. He was subsequently charged by the FTC with insider trading, found guilty, and sentenced to four months in prison.

Equifax's senior executives are not alone in being held responsible for failures in security. Recent research by Kaspersky Labs found that 31 percent of data breaches result in people losing their jobs, primarily in senior positions.

Source: Yahoo Finance

High profile examples of data breach include:

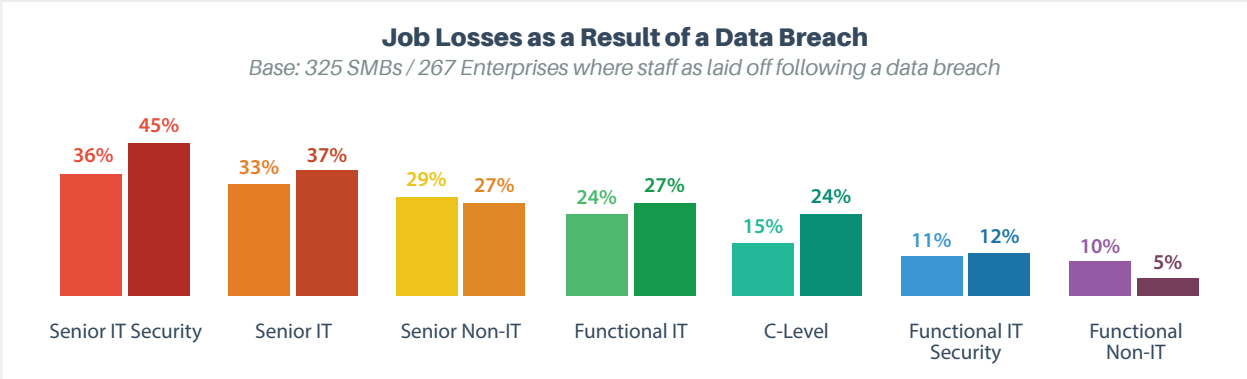
Target: The 2013 data breach started with malicious software on an HVAC contractor's laptop and resulted in the loss of 11 GB of user data on approximately 70 million consumers. Roughly six months later, their CEO, President and Chairman, Gregg Steinhafel, resigned from the company.

Sony Pictures: The 2014 attack, allegedly by North Korea, exposed IP and embarrassing emails sent by Sony's CEO, Amy Pascal. Within months, Pascal was pressured to resign.

Office of Personnel Management: The discovery in June 2016 of a breach at the U.S. Government's Office of Personnel Management (OPM) exposed highly sensitive 127-page Standard Forms (SF) 86 questionnaires used for background checks and security clearances on over 20 million people. Within days, the Director of the OPM, Katherine Archuleta, and its CIO, Donna Seymour, resigned.

Panama Papers: A 2016 breach of Panamanian law firm, Mossack Fonseca, exposed over 11 million highly confidential documents. Among those were documents showing that Iceland's prime minister, Sigmundur Davíð Gunnlaugsson, had sheltered money offshore. The public uproar caused the prime minister to resign.

Uber: A 2016 breach of personally identifiable information on over 50 million users and nearly 7 million drivers was kept secret for over a year. Once disclosed, the company fired its Chief Security Officer, Joe Sullivan, and Legal Director, Security & Law Enforcement, Craig Clark.



Source: Kapersky

Implementing security measures to avoid data breaches

While breaches will inevitably lead to "blaming and shaming", smart security professionals want to ensure that they are following security best practices to protect customer data and trade secrets. A good benchmark for this is to enforce "reasonable" security measures.

After breaches, several organizations have had action taken against them under Section 5 of the FTC Act. In many cases, the FTC argues that these organizations did not employ "reasonable" security measures such as those outlined in NIST 800-53.

> "Companies must maintain reasonable procedures to protect sensitive information. Whether your security practices are reasonable depends on the nature and size of your business, the types of information you have, the security tools available to you based on your resources, and the risks you are likely to face."
>
> - **Federal Trade Commission Guidance**

Best practices to ensure software security

Rather than implementing a complete compliance program with the NIST Framework, the FTC requires at a minimum the following steps to block cybercriminals from gaining access:

Risk assessments: All systems processing sensitive data should be evaluated to identify risks and threats. This makes sense, as organizations cannot defend against a threat of which they have no knowledge. Conducting a risk assessment or threat modeling will identify issues and allow security teams to plan accordingly.

Implement technical and physical safeguards: Once risks are identified, technical controls must be enumerated for each and assigned to software engineering, security, or operational personnel. Standardizing these through organizational security policies simplifies long-term monitoring and maintenance.

Security training: This includes training for both secure development and general information security. While annual, event-based training may ensure compliance with regulatory standards like PCI-DSS, ongoing, on-demand, or just-in-time training is more useful for knowledge retention.

Minimize data collection: You can't lose what you don't capture. A security-by-design plan minimizes the sensitive data captured and the associated risk of a breach.

Incident response plan: Breaches are inevitable, so forward-looking organizations have playbooks to follow in the event of a data breach. Build one and practice it.

Balancing delivery speed with software security

Securing applications and systems is possible without compromising on time to market. Through automation of proactive security processes, organizations can minimize manual efforts and enable security experts to strengthen security. They can also significantly reduce the need for remediation of vulnerabilities by integrating security early in the development process. This not only improves product security but also ensures timely release of software and saves costs. In addition, this allows management and auditors to have visibility into your security posture.

Neither your board of directors nor the FTC is demanding perfection. Residual risk will always be present. The goal is to understand the risk present in each application and to apply controls for risk management to a level appropriate for your organization.

Go fast. Stay safe.

SecurityCompass

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to adopt balanced development automation for rapid and secure application development. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on how organizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit them at securitycompass.com to learn more.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
995 Market St
2nd Floor
San Francisco, CA
USA 94103

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001