Brand security means endpoint security

By David Rozzio

11 Jan 2019

When British businessman Gerald Ratner, chief executive of a high street chain of jewellers, stood up to address the London business community in 1991, he had little idea that the next few minutes would wipe £500 million off the value of his company.

David Rozzio, Managing Director, HP Africa

By candidly describing the quality of goods sold at his shops as “total c**p”, Ratner prompted a mass consumer boycott and secured his own place in the pages of marketing textbooks for a generation – a case study on how to destroy a brand in seconds.

While CEOs may be more media savvy today, the risks to a brand’s reputation have never been higher. And top of the list of risks is cybersecurity – a disruptive force. Cybercrime is now a $600bn problem globally, and showing no signs of abating. The right security keeps your business running, helps ensure consumer trust, and avoids scrutiny by the government, media, and other organisations. But poor security can wreak devastation on your firm’s standing, its operations and finances.

A data breach significantly damages a brand’s reputation, resulting in stock prices dropping an average of 5% and increasing customer churn by 7%, according to a 2017 Centrify study. The biggest costs, however, are associated with lost business, estimated at up to $110 million.

As we've seen from recent public backlash over data breaches, consumers are no longer willing to stand by and watch companies recklessly handle their personal information.

A demand for responsible data management

From British Airways and Reddit to MyFitnessPal and Ticketmaster, high-profile incidents in 2018 created demand for responsible data management across the entire network ecosystem. Two-thirds of respondents to an RSA Data Privacy & Security Report said they would blame the company for the loss of their personal data, not the hacker.

For brands, it should not take a crisis to inspire action, and organisations are beginning to realize it's time to do things differently. The future of their brand could rest on the unsecured printer down the hall or the phone in the hand of their newest employee.

To minimise the reputational costs associated with losing sensitive information now is the time for brands to re-evaluate and reinforce their security. And it starts with two critical considerations:

Endpoints are the new frontline in the cyber battleground

Unsecured endpoints, such as PCs and printers, are a significant liability and can put an entire network and all of the company's valuable data at risk. The reason? Poor security hygiene. Many printers are left unsecured or are not updated with the proper security policies. Hackers know this and frequently target printers. In fact, seven out of ten organisations report their endpoint security risk increased significantly during the previous 12 months, while trust in antivirus software dropped considerably.

Today's IT threats strike businesses from many places and from all angles. Security must cover every entry point with multiple layers of protection. Embedded security in endpoint devices is an investment that small business and enterprises alike must consider to properly protect data, detect malware and recover potentially compromised data. For instance, both HP PCs and HP printers are equipped to thwart attacks before they start, with 'self-healing' technologies embedded in the machines that automatically install patch updates to ensure the device — and ultimately the network containing valuable data and information - is secure at all times.

Leave security to security experts

Security is not a place to take risks, especially as employee mobility and lifestyle shifts create new vulnerabilities with each device that enters or leaves the office. Ageing PCs with third-party security software and unsecured network printers now represent a high risk for many companies. With a proliferation of devices, many companies having a huge blind-spot in their security strategies, and don't realize that selecting the PC or printer to buy is actually the first security choice they must make. IT professionals have an opportunity to take the reins on this issue and protect their organizations.

A robust Device-as-a-Service (DaaS) subscription model enables a company to ensure adherence to security protocols and automatically update devices to keep them protected while reducing the time and labour required to manage them. DaaS also helps combat the risks of human error such as phishing or sending email to the wrong recipient, which accounted for 17% of security breaches last year.

With the number of connected devices dramatically growing, consumers and organisations alike are producing and consuming an increasing amount of valuable data - making devices at the edge vulnerable and attractive targets for security breaches.

Analyst firms like IDC tell us there will be up to 80 billion connected devices by 2025. Yet every 4.2 seconds, a new piece

of malware emerges.

In this context, every technology decision is a security decision, and ultimately, a decision about the future of a company's brand. Your customers, your employees and your entire supply chain demand you act as a responsible steward of their data, treating personal information with scrupulous sensitivity and stringent security protocols.

Is your brand living up their expectations?

ABOUT THE AUTHOR

David Rozzio is Managing Director at HP Africa