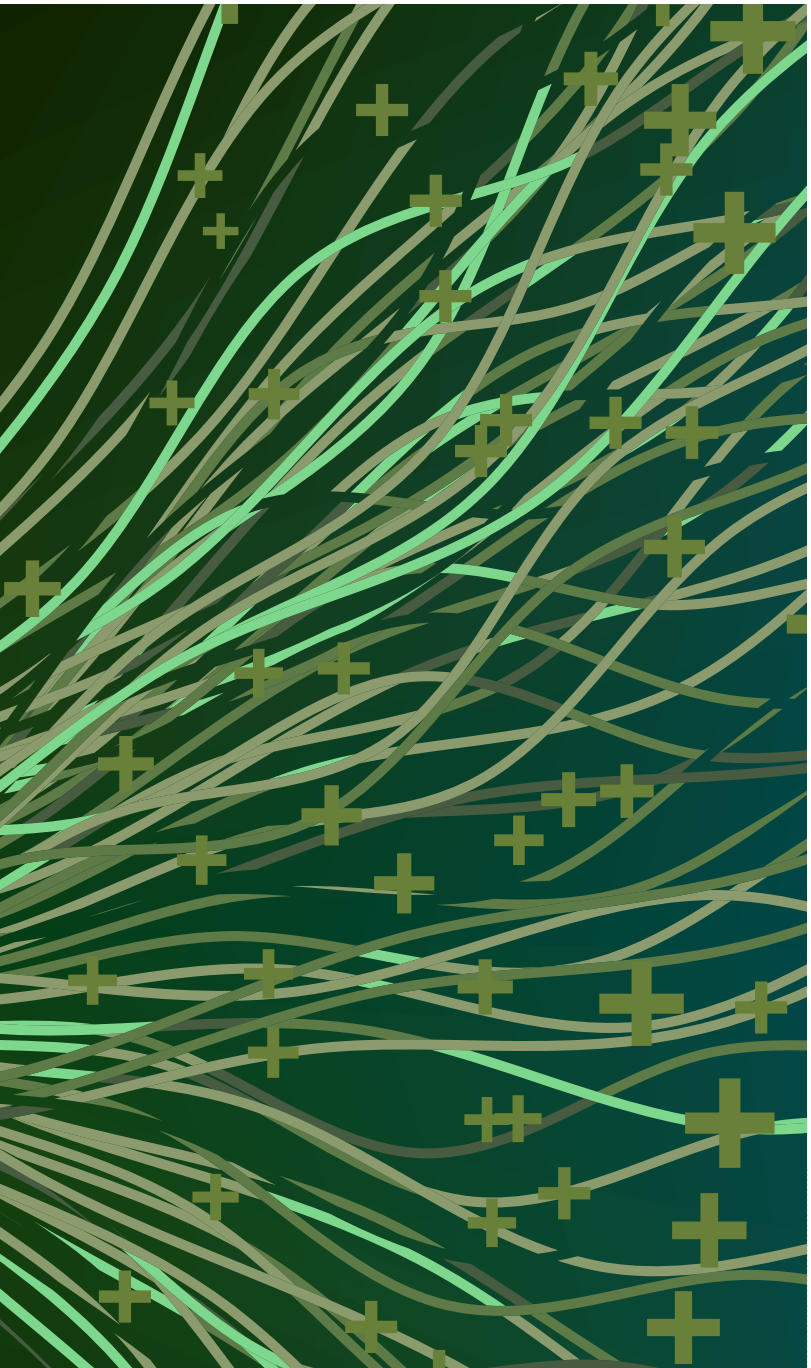
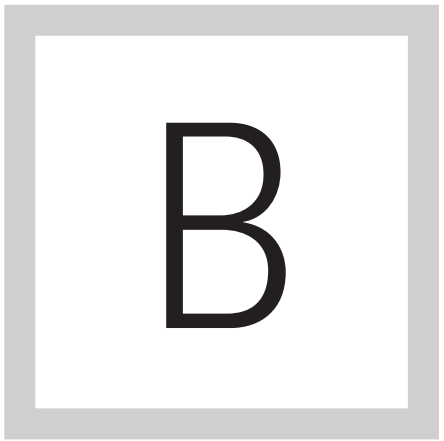


E-Guide

IMPROVE DATA PROTECTION WITH FORESIGHT, ACTION

TechTarget | SearchSecurity



ETTER DATA PROTECTION demands foresight and concrete action. Learn why breach training, monitoring and early detection capabilities can minimize damage when hackers attack.

IMPROVE DATA PROTECTION WITH FORESIGHT, ACTION

David Sherry

It's 2015, and it's not a stretch of the imagination to say that the majority of the population has either been a victim of a data breach or at the very least knows someone who has. With so many breaches of users' data, the inevitable question arises: "What will they do with my data?" The usual follow-up question is when will they use the data? The first part is easy; the second more difficult.

WHAT'S DONE WITH THE DATA, AND WHEN?

Compromised data is used in a wide variety of ways. It can be used for identity theft, credit card purchases, access to other accounts and to apply for credit in your name. It can also be used for ransom payments, threats and intimidation, be posted on public sites for embarrassment, used as blackmail and competitive advantage, or sold on the black market.

It should be noted that compromised data may not be used as soon as it is breached. While some breached info may be instantly used (credit cards used for purchases, for example), other data may be held for some time.

Social security numbers may be held to later use in identity theft (sometimes many years later) or may be parceled out for sale or trade, at which point the cycle of misuse may begin again. Large breaches of email accounts may be held for future spam and phishing attacks, which are becoming an easy attack vector for cybercrime.

HOW TO RESPOND

So what can be done to prevent or respond to this? First, ensure that you have a robust, scalable and holistic security function; that is key. This includes executive leadership, planning, implementation, architecture, staffing and incident response. Each of these elements plays a significant role in a successful security function, and the lack of one may increase risk. For example, without executive support, getting approval for funding, staffing and strategy can be more difficult. Without an incident response plan in place, security incidents can quickly escalate.

Recent breaches at Sony and the U.S. Office of Personnel Management indicate that their security postures were not as robust as they should have been. We should take their stories as lessons to be learned. It can be argued that security was not a priority in their organizations. After all, they both had

Home

Improve data protection with foresight, action

prior security events and were questioned on their posture previously, but no actions or improvements were undertaken. The lesson? Always perform a full review of security incidents and ensure that the necessary improvements are made promptly. In addition, be constantly assessing your policies, processes and infrastructure. Judge these against current best-in-class solutions, such as next-generation firewalls, advanced persistent threat defenses and log correlation and alerting solutions. Just because you have established a secure baseline, you must constantly evolve your defenses as the threats evolve.

THREE ACTION POINTS

Let me leave you with three points to focus on: Do all that you can to ensure early detection; have methods to observe exfiltration of data; and train for incident response.

Many, if not all, of the major breaches and compromises of the last few years have shown that the attackers had access to the networks and data for a great deal of time before detection. Some determined that they were compromised for two years or more! The longer the attack goes undetected, the greater the damage.

This makes it critical to have methods in place to observe when data is leaving your network, both in large datasets or through continued exits to non-network IP addresses. Knowing your baseline as to what is normal traffic is key to determining anomalies.

Finally, we all know that security events are a way of life, and that a big one can occur at any time. During an attack is not the time to be tweaking, testing or developing your incident response plan. Ensure that the talent and support you need are aware of their roles and duties, fully trained and tested, and that no instruction is necessary. Only with a well-developed and practiced plan can you identify, contain and eradicate the attack, and return to normal business as quickly as possible.

The attacks will continue unabated as long as they continue to be successful. We can take steps to reduce the possibility of a security incident, but also need to be ready to identity and address them expeditiously as well.

AS CHIEF information security officer of Brown University, David Sherry is charged with the development and maintenance of Brown's information technology security strategy, IT policies and best practices, security training and awareness programs, as well as ongoing risk assessment and compliance tasks. A CISSP and CISM, Sherry has 20 years of experience in information technology. He previously worked at Citizens Bank where he was vice president for enterprise identity and access management, providing leadership for compliance and security governance.

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.