Updates
September 18, 2017
Give Your Customers the Gift of Security

2017 has reminded us that data security threats continue to evolve and that the stakes for companies can be very high if their data security programs fail to evolve as well. Before the recent announcement of Equifax's megabreach, the year was characterized by an increasing drumbeat of smaller, targeted attacks. The year started with the annual rite of tax season phishing attacks designed to defraud front-line HR or finance personnel out of employee tax information, so-called "whaling" attacks because of the size of the "phish." A successful attacker garners the information necessary to file a fraudulent tax return and claim an employee's refund for himself. Appearing first in early 2016, over 200 organizations fell victim to the scam in 2017, a fourfold increase.

Ransomware attacks also spiked in both number and scope. WannaCry burst onto the scene in May, shutting down thousands of organizations around the world and reportedly causing over $1 billion in damage. But WannaCry was just one high-profile example of a plague of attacks that have risen 250% in the first portion of 2017, affecting a new business every 40 seconds. In some of these cases, the attacker also accesses sensitive data (or that can't be ruled out) and thus data breach reporting requirements come into play as well.

While these emerging threats pose new challenges for companies, they do not eclipse the threat companies still face from traditional hacking which, as we have been reminded this month, can have consequences that are both substantial and long-lasting. Equifax's recent announcement that it had lost data on 143 million people cut $2 billion from its market cap and has already spawned a host of class actions and government investigations. The consequences will no doubt extend for years. Nearly four years after suffering a breach during the 2013 holiday season, Target continues to incur staggering costs, settling in May with 47 states for $18.5 million in an agreement that also imposes a variety of ongoing security and oversight requirements. This settlement is in addition to Target's settlements with Visa ($67 million), MasterCard and a class of issuing banks (totaling $59 million), and consumers (totaling $17 million and currently held up on appeal over class certification issues). Target stated in May that the total cost of the breach to date has been nearly $300 million, with insurance covering about a third of the costs.

As companies prepare for this holiday season, the threats are more diverse and sophisticated, and the stakes are higher than ever. Effective data security is therefore as important as ever, and companies must make sure the fundamentals of data security are covered.

- **A holistic, company-wide data security program.** To create a comprehensive data security program, designate responsible officials and develop policies and procedures covering crucial security issues, including an incident response plan. Train employees regularly, raise their awareness of current threats and test your systems for vulnerabilities.

- **Vendor and service provider security.** Border walls alone do not provide effective security, and yes, we're still talking about cybersecurity. Modern networks integrate and embed third-party applications and services, bringing vendors and service providers inside the firewall. Similarly, companies increasingly send their most sensitive data outside their firewall to take advantage of cloud-based services. How can companies secure their data and minimize their risk despite the involvement of third-party vendors and service providers? Conduct effective diligence regarding vendors' data security policies and practices, and appropriately allocate risks and obligations via contractual provisions.
- **Insure against risk.** While companies can implement an effective security program and manage vendors and service providers to minimize risk, in today's threat environment, they cannot eliminate risk. Even the best-secured companies are sometimes Targets (pun intended) of highly-resourced and sophisticated actors. Manage residual risk with effective cybersecurity coverage. But buyer beware: cybersecurity policies can be fraught with exceptions and loopholes. Obtain expert counsel to make sure you're getting the right coverage at the right levels.

Of course, all of this is easier said than done, but if companies start early and leverage expert external resources where appropriate, the holidays can be filled with record-setting revenues and good cheer rather than haunted by the ghosts of data security incidents past, present and future.

Authors

Explore more in

Privacy & Security Retail & Consumer Products Apparel & Footwear

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality’s Voter ID Law