SF BLOG

SEEK TRUTH, FIND RESILIENCE

KNOW THYSELF: TIMELESS ADVICE FOR CUTTING-EDGE DATA SECURITY RISKS

Stroz Friedberg
October 12, 2016

Insider threats to intellectual property, managing information security across hundreds of third-parties, reliance on the Cloud and other technologies to push a business to a new frontier—these are some of the newest and most challenging risk factors to data security today. These risks shift with every new hire, fire, partner, and technology. General Counsel and security professionals must be able help organizations infallibly protect their most valuable data in spite of this changing landscape.

Here, Paul Schwartz, Professor at the University of California Berkeley School of Law and co-organizer of the upcoming Privacy + Security Forum October 24-26, in Washington, D.C., speaks about these critical, modern day risks with James Aquilina, Senior Executive Managing Director at Stroz Friedberg and co-chair of the Data Security Intensive Day at the event, and fellow event organizer Daniel Solove, Professor at George Washington University Law School.

Paul: James, let's start with insider risk—that's often overlooked because of political sensitivities, and simultaneously, it's a significant focus of new technology. What's one of the biggest areas of concern regarding this risk today?

James: Increased risk regarding employees who are internally-facing. One recent matter involved an IT staffer, who had fairly broad access to data in the organization, and his girlfriend, who was an executive assistant to a senior executive. The IT staffer was terminated due to business requirements, and then he and his girlfriend attempted to exfiltrate embarrassing information about several executives. And they actually did try to monetize that information against the business. Insider risk is becoming a lot more prolific from unwanted resignations, creating risk with respect to intellectual property, reputational harm or business interference, and business obligations. But whether it's workplace violence, misconduct, mental health or substance abuse – all of these comprise insider risk – companies are not always well prepared to address the risk. As a result, companies are starting to think a bit differently about how to protect themselves, and that manifests through advanced technologies, enhanced monitoring, and regulation of permission and access controls.

Paul: Dan, how proficient are businesses at managing permissions and data access controls?

Dan: A lot of businesses don't have a great handle on what data they have and who has access to it, nor a particularly good way of monitoring and controlling this access. The answer is coming up with an understanding of what data various people should have access to and then implementing that so it doesn't cause too much inconvenience, making it hard to run the business.
But for a lot of companies that initial step of learning what data they have and who should have access to it hasn't been done. Many businesses don't know themselves particularly well. Know yourself. That's

a key tenet businesses need to embrace to get a handle on this risk.

Paul: Companies must share information with other businesses to meet their goals. How should they manage third-party risk?

Dan: Vetting—a lot of businesses need help making sure they choose reputable vendors that have good practices. Often at large, complex organizations many different people contract with, and provide data to, vendors, and oftentimes there's no centralized vetting process. The risk comes down to whoever is the weakest link. If you give data to a vendor and it has poor security, then you have poor security, because you could be liable for that risk. Coming up with a consistent policy is key. Everyone who contracts with a vendor should understand what to look for when vetting them and have appropriate contractual provisions in place. Again, "know thyself" is a big first step. Understand who has what data, who is giving the data to the third parties, and then make sure everyone knows what to do regarding resources and process.

James: Also, avoid exception handling. It is common for businesses with long-standing relationships with vendors not to review those relationships for improvements in data security controls. Similar to when the C-level executive wants "super user" permissions to remotely access the environment from their vacation home. The same is happening with legacy vendors, and it's creating unnecessary exposure. Another issue is how companies are leveraging cloud providers. They do not always know how to set up a virtual private cloud inside the provider's environment, for example, so they contract with a third party for help. If the helper is not properly administering settings as resources come online, risk is created, and usually that risk is only identified after a breach.

Paul: Do you think innovation and security are at odds?

James: Many more businesses, small and large, are migrating to cloud solutions like Microsoft 365 and AWS, and using technologies like JIRA, Confluence, and corporate Dropbox. The problem is you cannot entirely disavow responsibility for administration. And this creates other kinds of risk, often business and litigation risk. In the face of an SEC subpoena, for example, if you cannot either extract or explain why you cannot extract all responsive data from your cloud repository, that's a problem. I cannot tell you how many businesses have created risk for themselves by improperly leveraging these types of innovative technologies.

Dan: One thing that's often overlooked: Good privacy practices reduce security risk. The United States Office of Personnel Management kept a lot of information much longer than they needed to, but one thing they didn't keep was information about families. It's a good thing they didn't, because that would have made for a much greater magnitude of risk. When you have a lot of stuff sitting around and you don't know who has access to it or what people are doing to it—that's where you lose control over third-party relationships. That's where everything starts to break down.
If you have good privacy practices, you'll reduce your risk. But there's a limit to what you can do. Because if you want to be fully secure, don't connect to the internet and don't have employees.

https://blog.strozfriedberg.com/know-thyself-timeless-advice-for-cutting-edge-data-security-risks/

***
Join the Stroz Friedberg team at the Privacy + Security Forum later this month in D.C. On October 24, James Aquilina and Scott Weber will lead a Data Security Intensive Day. Other sessions featuring Stroz Friedberg speakers take place over the next days, including a session on "Forensics: A Weapon and Shield in Data Breach Litigation." Click here to register for the event. We look forward to seeing you there!