JANUARY 15, 2015

InsideCounsel.com

BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS



A new cybersecurity reality for new media companies

General counsel are uniquely positioned to drive cross-organizational approaches to preventing, reacting to and minimizing risk

BY LI ZHU, ANDREA L. GOTHING, SETH A. NORTHROP

For the third time in as many of years, Sony is facing another data security breach — a nightmare that Sony probably thinks instead belongs in its most horrifying movies and video games. Sony's failings serve as yet another warning shot for media companies facing an ever-increasing collection of cyber threats. New media organizations are particularly vulnerable: They are often in the business of producing controversial content that may attract the ire of hacker groups. New media relies on the interconnectivity of digital platforms to deliver content and connect with customers. Finally, new media is often highly sophisticated at gathering and analyzing personalized consumer data, leaving a potential treasure trove for hackers. Most alarmingly, the Sony breach shows that hacking media organizations may not just be about stealing personal or trade secret data (such as those directed at other industries), but may instead be motivated by revenge and designed to cripple the organization by inflicting substantial technical damage.

For new media companies, securing corporate assets is no longer a topic relegated to server rooms of IT departments. Instead, highly publicized hacks have thrust the issue into boardrooms and C-level suites. As a result, general counsel increasingly have the responsibility and are held accountable for protecting the organization's precious data. Fortunately, inside counsel is well-positioned to make cultural and institutional changes to prevent and, more importantly, react to a breach.

Preventing the breach

Although preventing a breach is exceptionally difficult, general counsel can drive a number of initiatives to decrease risk for the organization.

1. Coordinate with compliance and IT to develop effective security policies

Protecting the security of an organization requires cooperation at all levels. The IT department should not be alone in navigating the complicated (and constantly changing) regulatory and legal minefield. Counsel can coordinate legal, regulatory and technical expertise to develop policies that both prescribe best practices and ensure execution by members of the organization. Consider enhanced multi-part authentication requirements for external access, regimented handling of vendor communications and distributed updates, strict data access restrictions, defined document retention guidelines, mandating regular review of resources such as the national vulnerability database, and ensuring third-party contracts are consistent with internal policies.

2. Compartmentalize responsibilities and systems

Breaches often originate from the inadvertent actions of individual employees or from individual systems. General counsel can substantially shore up security by insisting that IT systems be segmented and that individuals' access be highly compartmentalized. This compartmentalizing includes restricting access to certain information based on a user's "need to know" basis for their job function. Such a structure may be more complex for management, but it ensures an isolated breach (caused by an individual employee or system) will not proliferate throughout the organization.

3. Conduct regular, independent stress tests of the organization's security infrastructure

Independent stress tests are one of the most effective ways to keep the organization secure. This means conducting systematic penetration tests, where the company attempts to break through its own security, and auditing the environment to ensure compliance with industry standards such as ISO/IEC 15408.

4. Educate

General counsel are well-positioned to develop and implement data security training for the organization in conjunction with existing data retention and discovery training. This initiative should remind employees that what they include in their emails could one day appear on a hacker's website, identify pertinent security risks, and reinforce corporate regulatory obligations.

5. Insist on and act upon audit recommendations

Organizations often conduct security audits, but later fail to plug security loopholes identified in the resulting recommendations. General counsel are well positioned to ensure that these recommendations are executed.

Responding to the breach

Given the scope and repercussions of the Sony breach, new media companies should recognize that even sophisticated and presumably well protected systems can be breached. Therefore, the general counsel must focus on the organization's ability to respond to a breach, in addition to prevention. This response must, however, rest on more than merely scolding the media on its decision to publish stolen information. By leading a more comprehensive approach, the general counsel can limit corporate legal risk and avoid the long-lasting public embarrassment suffered by companies that have been breached to date.

1. Deploy tools for detecting security abnormalities

Given the continually evolving technical risk, it is important that tools be capable of detecting abnormal system, user and data patterns within the network. Data theft often continues for days, weeks or even months after a breach. Early detection of these

[InsideCounsel].com
BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS
JANUARY 15, 2015

telltale signs can limit the organizational exposure and allow a more effective response.

2. Create a rapid response team

Each organization should create a team charged with responding to the "nightmare" scenario of a data breach. Ideally, such a team should include inside and outside counsel, members of the compliance team, public relations representations and members of the technical team. Clearly defining responsibilities before a breach can minimize panic following a breach and speed up precious response time. Further, by involving outside counsel, the organization may be able to leverage attorney work product and privilege protections as they react to the breach.

3. Ensure company policies comply with federal and state regulations

The full scope of applicable regulations is beyond the scope of this article. However, general counsel can substantially limit corporate risk by ensuring the organization's data collection, security and privacy policies — along with the breach response strategies — are implemented in compliance with applicable regulations. By doing so, the potential legal risk during inevitable post-breach litigation will be substantially minimized.

Cybersecurity threats promise to be one of the most difficult challenges facing general counsel going forward. Security will be particularly challenging for new media companies engaging the world through increasingly interconnected platforms. General counsel, however, are uniquely positioned to drive cross-organizational approaches to preventing, reacting to, and minimizing the risk to the organization.

About the Authors

Li Zhu
Li Zhu is an attorney at Robins Kaplan LLP. He assists clients with complex technology-centric challenges including intellectual property, business, cybersecurity, and privacy litigation. lzhu@rkmc.com.

Andrea L. Gothing
Andrea Gothing is an attorney at Robins Kaplan LLP. She assists clients with complex technology-centric challenges including intellectual property, business, cybersecurity, and privacy litigation. algothing@rkmc.com

Seth A. Northrop
Seth Northrop is a trial attorney at Robins Kaplan LLP whose practice focuses on intellectual property and global business and technology sourcing. He has substantial experience with complex business litigation involving various technologies including software and hardware design, analytics, networking, database, and E-commerce systems. sanorthrop@rkmc.com.