NATIONAL SECURITY LAW JOURNAL

Excerpt from Vol. 5, Issue 1 (Fall/Winter 2016)

Cite as:

Chelsea Smith, Alexandra Diaz, and Richard Sterns, Symposium Tabletop Exercise, *Data Breach at a University: Preparing Our Networks*, 5 NAT'L SECURITY L.J. 121 (2016).

ISSN: 2373-8464

The *National Security Law Journal* is a student-edited legal periodical published twice annually at the Antonin Scalia Law School at George Mason University in Arlington, Virginia. We print timely, insightful scholarship on pressing matters that further the dynamic field of national security law, including topics relating to foreign affairs, intelligence, homeland security, and national defense.

We welcome submissions from all points of view written by practitioners in the legal community and those in academia. We publish articles, essays, and book reviews that represent diverse ideas and make significant, original contributions to the evolving field of national security law.

Visit our website at www.nslj.org to read our issues online, purchase the print edition, submit an article, or sign up for our e-mail newsletter.

SYMPOSIUM: TABLETOP EXERCISE

DATA BREACH AT A UNIVERSITY: PREPARING OUR NETWORKS

Summary Prepared by Chelsea Smith, Alexandra Diaz, and Richard Sterns*

On Wednesday, April 13, 2016, the Antonin Scalia Law School at George Mason University, the Law and Economics Center, and the National Security Law Journal co-sponsored a full-day cybersecurity tabletop legal exercise entitled, "Data Breach at a University: Preparing Our Networks."

OVERVIEW

On Wednesday, April 13, 2016, the Antonin Scalia Law School at George Mason University, the Law and Economics Center, and the National Security Law Journal ("NSLJ") co-sponsored a full-day cybersecurity tabletop legal exercise entitled, "Data Breach at a University: Preparing Our Networks." The event included 45 participants from the Department of Homeland Security ("DHS"), Department of Justice, Department of Defense ("DOD"), Department of Education, state governments, private sector partners, the Multi-

* Chelsea Smith, Editor in Chief, National Security Law Journal; Alexandra Diaz, Executive Editor, National Security Law Journal; Richard Sterns, Managing Editor, National Security Law Journal.

State Information and Analysis Center ("MS-ISAC"), University of Maryland, and George Mason University. The exercise consisted of four scenarios of data breaches involving universities. The scenarios, crafted by experienced cybersecurity professionals, allowed the participants to explore issues pertaining to data breaches involving the loss of personally identifiable information, cyber intrusions involving companies that have contracts with the government, the exfiltration of sensitive research, attacks on .mil networks, and ransomware.

OBJECTIVES

While the exercise centered on data breaches involving universities, the event had a broader goal of focusing on how lawyers can better understand their roles, responsibilities, and duties in response to cyber incidents. The opportunity to bring together a wide range of diverse professionals to seek concrete cybersecurity policy improvements was also an underlying objective.

The four overarching goals for the exercise were as follows:

1. All participants would develop a greater understanding of the various actors at play upon the occurrence of a significant cyber incident, including the roles and responsibilities of various federal agencies, and the capabilities of private sector organizations. Attorneys for the federal agencies and the private sector would have a greater understanding of roles and responsibilities in information sharing and incident response following the identification of a cyber incident.
2. Attorneys for federal agencies would develop a deeper knowledge of their agency's protocols for addressing and responding to data breaches. They would also brainstorm ideas for improvements to these protocols, including identifying areas where current protocols may be deficient or lacking in adequate guidance.
3. Attorneys for federal agencies and private sector entities would have a greater appreciation of how the contractual

relationship that defines their interactions governs data breaches. They would also understand where beneficial changes might be made to these types of contracts and the relevant statutory and regulatory issues at play in attempting to alter these contractual relationships.

4. Attorneys for the Coast Guard, the DOD, and DHS would have a greater understanding of how data breaches effect the .mil and .edu environments within their jurisdiction and how they can respond to those breaches. They would also understand where improvements to departmental policy may be made and which areas are most ripe for beneficial change.

SUMMARY OF DISCUSSION

Key points raised in the discussion include:

- Universities, like many companies in the private sector, often have a mistrust of government, particularly when responding to data breaches. However, universities, and others in the private sector, need to have a solid understanding of the broader context of cyber threats, and of the government resources that are available to help if they are willing to seek them. By engaging a larger community of partners, both in the public and private sectors, universities and other institutions may be better able to address the threat(s) that they face and build a more trustworthy relationship with government agencies.
- University networks are often decentralized and include many different networks. Chief Information Security Officers ("CISOs") in universities generally do not have a comprehensive view of their network(s), making identifying data breaches more difficult. Universities must manage a constant tension between facilitating an open network environment that promotes academic freedom and

maintaining quality cybersecurity. Universities, as a consequence of their missions to provide the highest quality education to their students, foster a robust "bring your own device" environment and the institution is incentivized by faculty to avoid restricting their access to data and research.

- Some universities have direct access to the Department of Education's outsized data systems with enormous amounts of valuable information such as the financial aid information of students. Further, many institutions of higher education are beginning to connect their systems, effectively broadening their networks into small cyber-cities and potentially creating more vulnerabilities.
- Many universities lack the privacy offices common in large corporations with huge amounts of personal information and instead utilize resources across multiple program offices to ensure compliance with state and federal law.
- Despite this increasingly complex environment, many universities lack cybersecurity response plans and those that have one in place underutilize it. This is not unique to universities and applies to most companies in the private sector. In addition, government agencies are in the midst of revising incident response plans and carefully reviewing protocols following the U.S. Office of Personnel Management data breach discovered in June 2015.
- Key elements of successful data breach plans include: mechanisms to connect technical personnel attempting to repair a network with policy, legal, privacy, and public affairs professionals who all have unique roles to fulfil; policies on notification, and the content of notifications given to students, professors, and other stakeholders; established plans to offer credit monitoring, and other mitigation options; plans to create call centers that can handle the inevitable flow of

questions; and, regular training exercises practicing implementation of the plan.

- Discussions were held about the appropriate time for a university to contact law enforcement; when remediation of compromised networks should take precedence over a law enforcement inquiry; when attribution questions should be explored; and when notice should be given to regulators, government officials (such as a Governor's office and individuals impacted by the breach).
- CISOs attempt to segment networks to prevent lateral movement throughout the network. Minimal resources mean that the universities must manage risk and prioritize cybersecurity along with other school necessities. DHS established Memorandums of Agreement with various partners (including those dependent on industrial controls systems) to allow for quick response/remediation assistance. Something similar may be established with universities.
- DHS Centers of Excellence ("COE") are set up under public service grant authority, requiring information generated by the COE to be made public. If a breach occurs, DHS does not instruct the COE how to respond, but DHS is allowed to engage. Grant sections have been used for physical safety for some COEs. This requires the COE to implement and share a safety plan that DHS may provide feedback on with options to address any deficiencies. Similar clauses can be used for cybersecurity, requiring the university to maintain certain cybersecurity response plans.
- Special contracting relationships must be established for research universities to accept sensitive and/or classified research. Many research institutions are not interested in classified research because it is expensive to establish and maintain the proper classified environment, and because

academics seek to publically disseminate and publish their work.

- Ransomware remains a difficult issue. The financial incentives favor the bad actors. Focus should be placed on reducing vulnerabilities (back-ups) and raising the cost of partaking in these activities for criminals.

CONCLUSION

The event met its goal of facilitating a dialogue between government agencies, universities, and private sector partners. George Mason University, the Antonin Scalia Law School, the Law and Economics Center, and DHS hope to partner and facilitate more tabletop events of this nature on a variety of national security issues in the future.