The Horde is Over the Gates and in the Tower: Defending Against a Discovered Zero-Day
By Christopher Land
Just over two years ago as summer was taking hold in Cape Cod, the Woods Hole Oceanographic Institution ("WHOI") uncovered a coordinated attack by a foreign entity; a so-called advanced persistent threat ("APT" for short) had breached its network and infiltrated sensitive research files. WHOI (pronounced Read more

How Knowledge Integration Platforms, AI and Machine Learning Help the Duty to Preserve
By Daniel Meyers, Salim Elkhou, and Joseph Pochron
The IT infrastructure of businesses today is no longer limited to behind-the-firewall servers and enterprise appliances from traditional providers like Microsoft and IBM. Modern employees demand the ability to access their workspace and collaborate with colleagues in dynamic, diverse environments that can be Read more

Addressing the Evidentiary Challenges in Proving the Authenticity of Digital Records
By Tim Reiniger
Distinguishing authentic digital records from those that are forged is a central evidentiary challenge in the digital environment. This concern is complicated by the untestable and ephemeral nature of digital data, the ease and pervasiveness of copying digital information, and ubiquity of network access to digital documents. Read more

New York Quietly Relaxes In Camera Review Requirement for Social Media Discovery
By Joseph Francoeur and Sean Geary
Why should the courts have to undertake the burden of evaluating in camera a party’s social media account to determine what information is relevant and discoverable? New York’s Appellate Division, First Department asked that very question in 2015. In Forman v. Henkin, the majority responded to the dissent’s Read more

Lessons and Practical Guidance from the Target Data Breach AG Settlement
By Aldo Leiva
On May 15, 2017, Target Corporation executed the Assurance of Voluntary Compliance¹ ("Settlement Agreement) with the Attorneys General of 47¹ states and the District of Columbia, thereby settling all civil claims that had been brought against Target by the Attorneys General, arising out of the Target Data Read more

****Editor’s Message****
We are concluding the eighth full year of publishing the Information Law Journal each quarter, continuing to welcome authors and readers from across the ABA. This issue again presents articles focusing on various aspects of leading-edge domestic and international practice in information, Internet, and emerging technologies law. Nearly 200 authors have written for the Information Law Journal and its antecedents. Six authors are writing here for the first time.

Our next issue (Winter 2018) is scheduled to be published in December 2017. All readers of the Information Law Journal may share their experiences and knowledge with their fellow professionals by writing an article. Every qualified submission within the scope and requirements as explained in the Author Guidelines will be published. The issue following the next issue (Spring 2018) is scheduled to be published in March 2018.
The Horde is Over the Gates and in the Tower: Defending Against a Discovered Zero-Day Cyber-Attack While Protecting Your Intellectual Property and Research and Academic Integrity

By Christopher Land

Just over two years ago as summer was taking hold in Cape Cod, the Woods Hole Oceanographic Institution (“WHOI”) uncovered a coordinated attack by a foreign entity; a so-called advanced persistent threat (“APT” for short) had breached its network and infiltrated sensitive research files. WHOI (pronounced “who-ee” by those who know and love it) was not the first, and definitely will not be the last victim in the international intrigue of cyberwars. Countries such as Russia and China are seeking intellectual property, trade secrets, government information, and research data on global hotspots. This attack occurred just as the US government declared cyberattacks a national threat and emergency. Executive Order 13694 of April 1, 2015. Attacks that are growing in size, sophistication, and number of victims.

Universities and academic research institutions are key targets of these attacks. They comprise a perfect storm of vulnerability and valuable information: great minds and big projects working under a strong and respected tradition of open academic process, and often with individualized networks without centralized IT control. Balancing the demands of an open access and transparent academic organization, while protecting national security interests, takes careful coordination, planning, and oversight. This article will provide suggestions on how to develop an action plan, how to roll it out, and how to weigh the competing needs and interests of an academic institution pulled into an international cyberwar.

When—not if—your company, research organization, or university has a significant cyber breach, planning and organizing the counterpunch will be your key priority. Assessing the damages can be done after the fact. For a private research and scientific organization such as WHOI, knowing what was accessed was secondary to knowing the extent of the breach, planning to stop and plug it, and then developing a solid rollout plan for recommended remediation and media fall-out. An attack from an APT is no mere “Nigerian bank” spam attack; an APT is a highly skilled hacker or team of hackers, sometimes sponsored by foreign governments, foreign military, and/or intelligence services. An APT intruder tries to get into your network, avoids any detection software system/s, and quietly lurks around creating back doors, new means of access, and rewriting codes to hide its footprints on how it may extract information. An APT can lie hidden, slowing moving around your system, trying not to trip any network security alerts by only having occasional and small extractions of data, while it explores and builds its own infrastructure in your network. Like a ninja, slowly building traps, hidden back doors, and holes in your organization without you knowing. It is insidious and menacing.
The attack on WHOI was a so-called zero-day vulnerability by an APT. A zero-day is an unknown threat to your software, hardware, or network that can create complicated and systemic breaches before anyone realizes something is wrong. It is a breach, from a sophisticated attacker, that is not yet publicly known or patched. WHOI was subject to a zero-day attack by an APT located in China. They were highly sophisticated and knew what they wanted and how to navigate the system. The attack resulted in significant media coverage and attention from local media, as well as NBC, Fox News, and the online Quartz magazine. See, Woods Hole Oceanographic Institution Says Hack Linked to China, NBC online (10/16/2015); Woods Hole Oceanographic Institution targeted by cyberattack, Fox 25 Boston News online (10/19/2015); One of America’s premier research institutions was hacked—and the signs point to China, Quartz (10/16/2015). If you suffer a zero-day attack or have a network vulnerability exploited by an APT, here I provide the steps and the questions we asked and suggest this might provide a framework for any entity.

Legal Take the Lead - Upon receiving notice from the head of WHOI’s IT, I brought the entire project under the command and auspices of the General Counsel’s office, with day-to-day management left to the head of IT and IT’s cybersecurity team. Changing a team’s project report structure can be no small matter depending on a company’s culture. But besides making certain action discussions subject to attorney-client privileges, it also provides gravitas to the issue, and third-party oversight that reduces the chances of an internal IT team hiding past mistakes, and a solid structure for mixed-asset, cross-team collaboration.

Know Your Response Team - The next call was to outside counsel who had experience in cybersecurity and national security matters. Luckily when I was still at a firm, I had worked with a partner with such experience, Gus Coldebella. Gus ran a task force on cybersecurity in the Department of Homeland Security before going into private practice. The point here is, know your cybersecurity team before “it” happens. Gus and I were on the phone five minutes after I got my initial call, and we were all meeting in my office the Monday morning after. Also, know your IT team; I try to meet with WHOI’s IT and the cybersecurity team once every two or three months to review security issues and developments.

Cyber Insurance: Buy It – According to one survey, less than 30% US companies have bought cyber policies, despite the increased assaults in the two to three years. Cyber Insurance Market Watch Survey, The Council of Insurance Agents and Brokers (10/26/2016). That 70% of American companies are exposed seems staggering considering the major news worth attacks on companies such as Target, Sony Pictures, Penn State, and the list goes on. There are plenty of good articles on the best cyber polices, and this is a still largely unsettled field of insurance that continues to quickly develop. Further, there are numerous options on such policies, and much the topic of options requires a much more involved review than can be addressed here in this article. Whatever your policy covers, however, make sure that it includes expenses for hiring outside IT consultants, a response team, cyber legal experts, and maybe even public relations firm. WHOI had not yet placed such coverage, for various reasons including cost, coverage was very unclear in 2014, we did not hold or retain third-party
Personally Identifiable Information, and therefore exposure and liability was unclear. As such, when the breach was discovered, we were scrambling to hire a third-party consultancy firm. If you have a policy in place already, then you should establish a rapport with the IT cybersecurity experts early, have regular calls, and see what proactive assistance they can provide. Despite not having a policy, our IT team worked quickly – within days – to get a cybersecurity consultant firm on site.

**Stay Dark and Assess the Threat** – Within days, the project task force team met to lay out our plan. With an advanced and sophisticated threat, we were advised not to begin remediation until the threat was known and uncovered completely; only then should we shed light on it. This process of knowing and uncovering the depth and level of the attack may take a couple of weeks. This means your system remains vulnerable.

Therein lies the risk balance. If the APT is not fully understood, back doors into your network could be left open and exploited when you think the system has been protected. But if the APT is left in your system while you hunt for it, you could be left vulnerable to extraction of more data and IP. We balanced this by leaving our system running, not indicating we had found the intruder, and watched the APT movements. We had protocols in place to shut down if the threat was after key data. In our case, if the APT set sights on Personally Identifiable Information (“PII”), or Sensitive Personal Information (“SPI”), or accessed sensitive intellectual property, we would take the risk and shut down the APT and any transfer of data immediately. WHOI develops cutting-edge robotics systems and autonomous vehicles, and data and research are our crown jewels of our IP and a hot industry. A thief could not be allowed to walk out the door with them.

To successfully manage this risk of loss of key data requires having a solid plan and protocol in place on when to stop the APT, due to the value or legal risk of the data being compromised compared to the risk of the APT knowing you have located them before you have completed remediation readiness. While pulling up the drawbridge too soon has the risk that not all backdoors have been located, you have to know when that risk weighs less than your property value or potential liability.

**Loose Lips Sink Ships (as does email and voicemail audio files)** – At the initial assessment we knew what we did not know: how many systems, files, directories, databases, and email systems were compromised. So, we initiated drastic secrecy security protocols. No emails about the project. No phone messages. Almost all communication was conducted via voice phone or encrypted systems with added security precautions.

In addition, we also kept to a minimum those who needed to know about the attack and the remediation plan. The bare minimum. We informed the Chairman of the Board and the Chair of the Audit and Risk committee, but no other board members. Internally only the project team (composed of IT, legal, and facility security), the Vice President overseeing IT, and the President of the Institution
were informed. No other VPs, departments, or leadership levels were briefed (except for two others carefully chosen, described below). The risk was too great.

This did carry some independent internal risk. As an academic research institution, the department heads (who head the various divisions) form the primary deliberative body of the Institution. In other words, while the Vice Presidents implement strategy and day-to-day management, strategy itself is typically bottom-up and driven by the researchers and scientists. Leaving them out of the process, thereby risking alienating the key constituent body who makes most institutional decisions, could again threaten levels of trust, but also undermines a successful rollout plan. To mitigate that risk, however, we briefed two senior researchers whose departments were at risk and apparently targeted in the breach (from what our initial IT assessments could indicate) and who had security clearances. This seemed like the best-balanced approach, given the situation. It was important to keep the circle small but include leadership who could be affected and who could add value and insight in perfecting a rollout plan that could affect the researchers. As with any new process, getting the thoughts on how a process – before it is actually implemented – could impact those it was is directed at is invaluable. The hypothetical issues raised by these department chairs and researchers were key in making a plan that worked.

**While IT Assesses, You Plan** – During our weekly meetings (which did not appear on our Outlook calendars or were given a false project name), IT and our IT consultants briefed us on what they learned and had been working on, and then we developed what our public rollout and remediation strategy would look like. This was no easy task for a research institution with scientists, engineers, students, and researchers in the field around the world. We had to overcome significant coordination hurdles to execute a major remediation event on one single day, globally, and within a few short hours. That was deemed necessary by the consultants because if a single user failed to update the systems or passwords properly and timely, the APT could re-enter the system. This required taking the entire network offline, with no warning, for six to twelve hours. Imagine being the person responsible for taking your organization’s entire network offline with no warning to any of its departments, divisions, workers, or researchers. You will want that to go smoothly.

IT developed a careful technical schedule for the offline remediation, laying out the steps to be taken, and when. But the technical aspects are just a small part of the problem; you also have the risk of a general panic and major disruption of operations. When remediation starts, there cannot be long wait and a busy signal for the help desk, unknown deadlines will be on that day and so the system has to be back up and running fast. Not only would a failure disrupt operations for potentially days or weeks, it could also destroy trust between operations and the program team. At WHOI, that damaged trust would be among our researchers and scientists, and it would not be quickly or easily repaired. Doing it right will be easier. We developed and prepared a number of actions/initiatives to be deployed at zero-hour:
- Staffed additional IT professionals (both from WHOI and with the contractor).
- Added operators and a phone bank to take calls and run people through the process of updating passwords.
- Developed procedures to confirm employees were validated and authentic.
- Created an internal landing page that would direct people to validate and then update passwords.
- Prepared a short but cryptic message for outside users attempting to access the internal the system.
- Drafted a media statement and media plan.
- Posted pre-printed informational flyers throughout the campus.

**Coordinate with Federal Authorities** – To many general counsels, inviting federal law enforcement or other interested entities may seem fraught with other risks. But this is an area where their expertise, assistance, experience, and knowledge can be a great help. You can balance to what extent you let them under the curtain if there is potential for compliance, liability, or regulatory issues, but some level of discussion or coordination is advised.

***

In the end, despite many worries that it would be a disaster, the remediation plan worked nearly flawlessly and with little concern or complaint. We have, by all accounts, successfully excised the APT and updated our systems, and we continue to monitor and upgrade. Less than two months after WHOI’s remediation efforts in October 2015, Chinese nationals were arrested for attacks on the federal government’s office Personnel Management. *Chinese government has arrested hackers it says breached OPM database*, Ellen Nakashima (Washington Post, 12/5/2015). And just this month, China’s Ministry of Education announced plans to further build its cyber expertise that would result in a so-called “Cyber Army.” ‘Cyber Army’: Beijing Raising a New Generation of Digital Wizards (Sputnik, 8/18/17). The cyber threat is never-ending, ever evolving, and only growing, but we hope that with good preparation, solid forecasting from leadership, and vigilance, we are even better prepared to deal with future threats.

Some other key takeaways I might share:

- **Turn attack into opportunity.** This is a good time to invest in needed cyberinfrastructure or changes. If your legal department has been pushing for increased IT infrastructure, IT security experts, or insurance coverage, use this as your cudgel. If there is a problem
department or area resistant to change, this can be the motivation and the argument for that change.

- **Coordinate at base level of the organization.** We brought in all lead supervisors of the administrative assistants the day before zero-hour to brief them and answered questions. We met at 4 p.m. the day before the rollout to mitigate the risk of an inadvertent leak; however, it also allowed them to know what was happening, to inform their teams, and to help roll out the program.

- **Tabletop and meet.** Running a breach exercise and discussion of these issues with your likely project team is priceless. Bring in your outside experts to do the exercises with you, it is worth the investment, to do it then and do not first meet in an emergency.

Christopher Land is General Counsel and the Vice President for Legal Affairs at the Woods Hole Oceanographic Institution. As General Counsel, he provides advice, opinions and representation on all areas of law affecting the Institution. Among his duties are engaging in institution strategy and business development; providing counsel and advice concerning compliance with federal and state statutes and regulations affecting research and higher education organizations; and negotiating, drafting and reviewing contracts.

He is responsible for providing proactive counsel on a broad array of critical, strategic, and public policy issues to WHOI’s Board of Directors, the Director and President, and all senior managers in their WHOI roles and positions. The size, complexity, scope, and diversity of the WHOI community generate a range of complex, cutting edge legal issues. Many, such as academic freedom, sponsored research, shared governance, and student rights and obligations, are unique to a research and academic environment. WHOI also has the added complexity of being a large maritime operator of oceangoing vessels, maritime crew, longshoremen, a number of small craft, AUVs and ROVs, and the resulting Admiralty Law and Jones Act issues. He also manages WHOI’s Risk Management and Compliance system.

Chris received a BA from San Francisco University and is a 2002 graduate; Order of the Coif and Cum Laude, of Tulane Law School. Mr. Land has been a senior attorney with the firm Goodwin Procter of Boston, where he represented clients in various industries, including pharmaceutical and medical device manufacturers, power and energy companies, and academic and research institutions, including WHOI.