UNIVERSITY of VIRGINIA | McINTIRE SCHOOL of COMMERCE

UV7351
Sept. 27, 2017

The Phoenix Project: Remediation of a Cybersecurity Crisis at the University of Virginia

Virginia Evans listened intently as the Board of Visitors (BOV) deliberated budgetary issues within the Board Room of the Rotunda, the centerpiece of Thomas Jefferson's Academical Village.[1] As the University of Virginia's (UVA's) chief information officer (CIO), Evans had been asked to attend the two-day meeting in case any questions related to UVA's information systems came up. The first day had been relatively uneventful, but then Evans felt her phone vibrate. A quick glance down revealed a message marked urgent—she was being asked to call UVA's chief information security officer immediately.

A few minutes later, just outside the Board Room, Evans learned the news that would turn her summer upside down. Federal authorities had discovered that possible nation-state actors had access to UVA's systems, and they could only guess at the cyberattackers' intent. During a break, Evans sought out Pat Hogan, UVA's executive vice president and chief operating officer, to inform him of what was going on. Together, they decided that the best course of action was to brief the BOV while its members were still in town. There was no question that this sudden news could have a dramatic impact on UVA's community at large, and quite possibly on Evans's career. There had been many examples in the news of both private- and public-sector CIOs who had their careers altered by cyberattacks. To manage the remediation effort successfully, Evans felt she needed to gain the BOV's support, not just financially but organizationally. The following day, that's exactly what she set out to do.

During a closed meeting on Friday, June 15, 2015, Evans advised the BOV that UVA's information systems had experienced a "major security breach." The BOV responded with a slew of questions: "What are they after?" "Are our students safe?" "Has any personally identifiable information (PII) been compromised?" While Evans could answer some of the questions, the answers to most would require a thorough investigation, and a planned, full remediation of the cyberattack. She promised to keep the BOV informed and report back at the next meeting. The next few months would be like nothing she had ever experienced.

The University of Virginia: A Top-Ranked Public University

UVA was a major public research university and the flagship academic institution for the Commonwealth of Virginia. Founded in 1819 by the third president of the United States, Thomas Jefferson, UVA was known for its historic foundations, student-run honor code, and secret societies. Throughout its history, UVA had won praise for its unique Jeffersonian architecture, with the original design revolving around the Academical

[1] This is a field-based case. All information and quotations, unless otherwise noted, derive from author interviews with the protagonist and other people involved.

Village and Rotunda—UVA's most recognizable symbol. The United Nations Educational, Scientific and Cultural Organization (UNESCO) had designated UVA as America's first and only collegiate World Heritage Site in 1987, an honor shared with Jefferson's nearby home, Monticello.[2]

Since its founding, UVA had continued its mission to develop future leaders who were well prepared to shape the future of the nation and the world—a testament to its original governing BOV, which had included Thomas Jefferson, James Madison, and James Monroe. In 2015, UVA comprised 11 schools in Charlottesville, Virginia, plus the College at Wise in southwestern Virginia, while offering 48 bachelor's degrees, 94 master's degrees, 55 doctoral degrees, and a number of other professional degrees. The institution was ranked in the top two public universities in the nation, accepting only the best students (around 90% of students admitted were in the top 10% of their high school graduating class) and those who showed the exceptional promise Jefferson envisioned. Approximately 22,000 students were taught by 2,800 full-time faculty, and were supported by just over 10,000 full-time staff.

UVA's total annual budget in 2015 was $3.07 billion. It was interesting to note that despite being a public university, less than 6% of UVA's operating budget came from the Commonwealth of Virginia. An additional 17% came from tuition and fees, almost 50% from medical patient services, over 10% from research and development of intellectual property, and roughly 12% from gifts and endowments. Numbers like these prompted some to call UVA a privately funded public university.

Information Technology Services (ITS)

In addition to its exceptional academic reputation, UVA was known to be a leader in its use of information technology (IT) within higher education. A central component in UVA's use of IT was the ITS organization, whose mission was to "be a trusted partner and strategic resource to the University community, aligning technology to advance the University's mission."[3] In 2015, ITS had 240 employees and an operating budget of $50 million.

Evans had served as UVA's CIO since February 2014. In her role, Evans was the leader of ITS, responsible for planning and coordinating central IT infrastructure, applications, and support, as well as information security, policy, and records management. Evans had over 25 years of IT experience, ranging from IT consulting with Andersen Consulting and independent IT consulting, to over 20 years managing IT at UVA at both the central and school levels. She held a bachelor's of science with a concentration in accounting from the University of North Carolina at Chapel Hill and a master's of science in management information systems from UVA's McIntire School of Commerce, where she had also served as an adjunct professor teaching business process-reengineering classes at the graduate level.

Cyberattacks: A Growing Threat to Companies, Agencies, and Universities

2014 was considered by many experts to be the year of the cybersecurity breach, and 2015 was shaping up to be even worse. Megabreaches, or breaches where more than one million records were stolen, had become common in the news. Private-sector companies such as Home Depot and JPMorgan Chase & Co. revealed that millions of their customer records had been stolen, while Anthem reported that PII had been stolen from 80 million of its health-insurance customers. In the public sector, a cybersecurity breach at the U.S. Office of

[2] "World Heritage List," UNESCO World Heritage Convention, http://whc.unesco.org/en/list/ (accessed Sept. 13, 2017).
[3] "About ITS," UVA ITS website, http://its.virginia.edu/about.html (accessed Sept. 13, 2017).

Personnel Management exposed more than 21 million citizens' PII, which included background-check information (e.g., fingerprints, financial histories, and so on).

Universities were also fast becoming a favorite target of cybercriminals and dangerous state actors—in large part because of their openness and decentralized nature. In fact, it was estimated that 25% of all security breaches took place in higher education. Pennsylvania State University (Penn State), Harvard University, Johns Hopkins University, Rutgers University, and the University of Maryland all suffered security breaches in the 2014–15 academic year. Universities could be a prime target because they often had significant research intellectual property and vast stores of PII and financial information, including payment information from students and tax information for employees. In 2015, Symantec reported that universities were the third most popular target for cybercriminals behind health care and retail, with cybercriminals targeting financial assets and intellectual property, and looking to acquire information that could be used for political motivations.[4]

Cyberattacks could be very costly to universities. For example, Penn State spent over $2.85 million to remediate a data breach in its College of Engineering,[5] and the University of Maryland's breach, which affected more than 300,000 current and former students, cost the university an estimated $3 million to recover and mitigate.[6]

At the time of the UVA cyberattack, the three most common attack methods were (1) spear phishing, (2) unpatched systems, and (3) zero-day exploits. Spear phishing had evolved from phishing, which involved sending millions of e-mails asking the victims to click on a malicious link or download an infected file. Over the years, criminals had started to select only a few victims in an organization, tailoring the e-mail messages to these employees, which was known as spear phishing. Spear phishing was an attack on human vulnerabilities and remained the most popular and effective attack vector. In 2015, on average, criminals sent spear phishing e-mails to 18 individuals within an organization they targeted. This tactic made it very difficult for the spam filters and automated phishing-detection systems to spot spear phishing.

The next typical attack vector was identifying and attacking computer systems that had not been patched properly. Patches were software updates installed on computers that fixed a known system vulnerability. Typically, software vendors such as Microsoft, Apple, and Adobe pushed patches on a regular basis. The amount and variety of software vendors that sent patches often made it difficult to manage all the updates to the computer systems. UVA's ITS managed several hundred servers for a variety of workgroups that ran a myriad of applications and services. Also, there were hundreds of computers used by university employees and hundreds more in student computer labs that needed to be constantly patched. Further complicating patch management was the fact that students, staff, faculty, and visitors could connect almost any Internet device to UVA's network. ITS had very little control over how and when these devices were updated with the latest security patches.

The last typical vector for attack was zero-day exploits, which were not publicly known and did not have a patch or workaround available to fix the security hole. The name "zero-day" came from how many days an organization had known about the vulnerability. Although rare, zero-day exploits were severe and very difficult to detect and mitigate. Typically, zero-day exploits were created and used by state actors or very sophisticated cybercriminals. In 2015, there were only 24 zero-day vulnerabilities reported.

---

[4] Symantec, "Internet Security Threat Report Volume 21," April 2016, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf (accessed Sept. 19, 2017).

[5] "Frequently Asked Questions," Secure Penn State, May 15, 2015, http://securepennstate.psu.edu/engineering-051515/faqs (accessed Sept. 19, 2017).

[6] Colin Campbell, "More Than 309,000 Identities Exposed in University of Maryland Cyberattack," *Baltimore Sun*. Feb. 20, 2014, http://www.baltimoresun.com/news/maryland/bs-md-university-of-maryland-data-breach-20140219-story.html (accessed Sept. 19, 2017).

The most common way to mitigate all three of these attacks was through a "defense in depth" IT security model. Defense in depth, or castle defense, was a layered approach originally conceived as a military tactic. The military defensive system typically used an outer wall to protect its citizens, a castle to protect more important resources, and a keep to protect the most valuable assets such as the king or queen. In an IT security context, a similar conceptualization was used, where the most sensitive information was identified and protected by many layers of systems. **Exhibit 1** shows the primary layers of defense that were in place at UVA at the time of the attack.

Layer 0, also known as "the kernel," included servers that held the most sensitive university data. Technological and process defenses were built around this layer so that only a few people and services could access the data. This protection technique was called hardening. The next layer of protection, Layer 1, included servers that employees and students could access using their log-in credentials (e.g., username and password), including e-mail servers, web applications, and so on. The final layer of defense, Layer 2, included all employee and student devices and local servers that held no sensitive information. In this layer, there was also a segmented area for research computers used by faculty and scientists at UVA that needed to be accessed from external organizations. No sensitive information was supposed to reside on these servers, and these servers could not access the rest of the UVA network. The ultimate goal of the defense-in-depth model was to harden the perimeter of the network while maintaining a secure kernel, detect unauthorized access to resources, and react to security incidents as they occurred. In UVA's case, the cyberattack had been detected by a federal government agency that promptly notified UVA's chief information security officer, who, in turn, contacted her boss, Evans.

The Rise of the Phoenix Project

When Evans left the BOV meeting, the first thing she did was call Mandiant, an internationally recognized cybersecurity firm. Coincidentally, she had recently attended a conference where she learned how Mandiant had helped Penn State navigate its cyberattack, and fortunately, she still had the Mandiant representative's card in her wallet! The second order of business was to get a contract signed with Mandiant, which cleared UVA's Procurement Office in record time. Evans exclaimed, "Responding as quickly as you can is important because you don't know what the attackers are doing!"

It was a pretty standard remediation contract, and Mandiant was on-site at UVA within 24 hours. The representatives came in with their own proprietary appliances that they attached to UVA's network servers to monitor activity and perform the necessary forensic work. Mandiant quickly discovered that two unauthorized attackers from China had been accessing the UVA systems, most likely through two unpatched systems, since April 2014. Based on experience, they knew that after gaining access, China-based cyberattackers tend to infiltrate as much as they can, moving laterally while infecting as many systems as possible. In addition to Mandiant, UVA leveraged Microsoft Services to focus on specific infrastructure components that needed to be monitored and remediated quickly.

Based on this initial assessment, it was clear that a high-level management team would be necessary to get the situation under control—particularly given that UVA's networks included the UVA Medical Center, an investment-management company that managed UVA's $5.3 billion endowment, and a patent foundation. With the help of Pat Hogan, Evans formed the Omaha team,[7] consisting of two members from the BOV, a senior communications representative, general counsel, enterprise risk management, the chief information security

[7] The name was derived from UVA's participation in the College Baseball World Series at the time the attack was detected; the World Series was played in Omaha, Nebraska.

officer, an external legal counsel, and herself. The Omaha team was responsible for providing executive oversight for the remediation effort from beginning to end.

Under the guidance of the Omaha team, Mandiant and Microsoft Services spent three weeks assessing the extent of the infiltration to scope the remediation requirement. They found that 62 servers had been compromised—some of which contained massive amounts of data. At that point, Evans knew that the remediation effort would be tremendous and require the attention of someone with vast experience managing large IT projects. The first person she thought of was Dana German, senior director for strategic projects and initiatives. With more than 15 years of experience leading and managing major IT projects in higher education, German had quickly moved up the ranks during her time at UVA, and she was well positioned to lead this effort.

Unfortunately, German was in the middle of a two-week vacation. At the risk of ruining German's vacation, and contrary to her previous instructions to "completely disconnect," Evans sent German a very brief but foreboding e-mail: *Hope you're having a great time! I need to meet with you on Sunday to discuss a high-priority matter.*

That Sunday, Evans and German met for coffee in a grocery store near their office building. German remembers the meeting well:

> After she briefed me on what had transpired over the past two weeks, Virginia told me to free up my calendar immediately. When I said, "Like Tuesday?" she said, "No, you don't understand—immediately." That's when the gravity of the situation really hit me.

The very next day, a covert project called Phoenix was initiated with German as the lead project manager. The Phoenix Project would be focused on the following high-level objectives:

1. Determine the extent of the intrusion. Although Mandiant had performed a preliminary investigation of the intrusion over the past several weeks, a more in-depth assessment was necessary to ensure that everyone had full information.
2. Develop a remediation plan. A detailed plan for addressing system deficiencies needed to be developed over the next few days, and given that the final remediation activity would involve bringing all UVA systems down to allow a new security system to be enacted, one of the very first decisions would be to schedule a go-dark phase.
3. Execute the remediation plan. Execution involved performing all necessary activities leading up to the go-dark phase, including:
    - tracking foreign attacker activities and responding as necessary,
    - developing methods of procedure (MOP)[8] to rebuild and protect critical applications and data on the compromised systems,
    - identifying all workstations impacted by the intrusion,
    - evaluating UVA's password-management system,
    - preparing to support end users during and after the go-dark phase, and

[8] MOP were step-by-step sequences of actions to be executed by maintenance/operations technicians performing an operation or action that implied a change of state in any critical component of an installation.

- communicating with all internal and external constituencies.

4. Harden UVA's defenses. Alongside all of the above, it was obvious that UVA's systems needed to be further strengthened to block further malicious activity.
5. Restore services. All systems would have to be restored and tested toward the end of the go-dark phase.

To accomplish these objectives, a large number of diverse personnel would be necessary. The challenges involved with identifying the necessary skill sets, "borrowing" the personnel from their assignments, and then organizing them into a high-functioning team were almost too much to comprehend.

Organizing a Stealth Army

In addition to the executive-level Omaha team, Evans and German initiated nine supporting teams at UVA and two external consulting teams—one from Microsoft Services and another from Mandiant. Finally, the federal government agency that originally detected the attack continued to be involved in an advisory capacity (see **Exhibit 2**).

The **Servers** team was responsible for confirming which servers had been infiltrated by foreign attackers, identifying all critical applications and data on the compromised systems, and constructing a concise master remediation list with all system names and changes that could be clearly referenced by all parties with ties to those servers. In each case, a retire-or-rebuild decision would be necessary. If a machine had to be rebuilt, an offline procedure had to be developed to make a seamless transition without affecting critical functions for the University.

The **Specialty Server Remediation** team focused on evaluating the effect of a cyberattack on UVA's faculty and staff e-mail systems. The members needed to ensure that compromised servers were identified and remediated properly, and to set up to prevent possible future attacks.

The **Network** team was charged with analyzing network segments for potential breaches. It had to help monitor attacker activity, set up separate network environments that could be used during remediation, and ensure that it was clear what was being turned off or kept on during the remediation weekend.

The **Workstations** team was tasked with helping with the investigation and remediation of workstations impacted by the intrusion and implementing monitoring devices on a subset of workstations.

The **Passwords** team was responsible for password management as part of the remediation activities. UVA had not previously *mandated* a change in user account passwords as part of end-user security hygiene procedures. The team needed to devise a plan for changing account passwords, making them stronger and having all existing user passwords expire at next log-in to prompt the creation of a new password. The team would also need to work with the User Support team to ensure that the volume of changes could be administered without issues.

The **Forensics** team focused on identifying intrusions and tracing them back to the source. They had to evaluate what the foreign entities were trying to access. Leveraging services from Mandiant, this team would need to monitor the environment continually throughout the project.

The **User Support** team focused on supporting end users after significant changes were implemented on the security front—for example, new password requirements. It was estimated that between 40,000 and 50,000

people would need to make the requisite changes immediately following their first log-in attempt after implementation.

The **Data Scanning** team was a combination of Mandiant personnel and UVA ITS staff. The team was responsible for examining every server and workstation that had been compromised or potentially compromised to determine what data were on the machine, to understand if any sensitive data had been exposed.

The **Communications** team was responsible for managing project communications from both an internal and external perspective. On the internal side, the team needed to ensure that a clear communications plan was developed and followed to address all stakeholders. This included communications to UVA's most senior levels (the BOV, vice presidents, and deans), all faculty, staff, students, retirees, and alumni. External stakeholders included the attorney general, the governor's office, the general public, and the press (e.g., the local newspaper and television stations).

The **Microsoft Services** team focused on specific infrastructure components that needed to be monitored and hardened quickly.

The **Mandiant** team provided support for the Forensics team, while also helping Evans and German formulate a remediation plan. Mandiant personnel were collocated with the UVA teams.

The **federal government agency** had an advisory role to Evans. It had originally alerted UVA's chief information security officer to the presence of attackers in the UVA network and was now there to help with high-level questions that the teams might have.

Given the large number of people involved (176 people in total), it was particularly challenging to maintain both agility and secrecy. Each new team member had to be sworn to secrecy before being "read-in" (i.e., briefed) on the project. To prevent others (especially the attackers) from knowing that a breach had been detected, all communication was done outside of UVA's systems, using Google Gmail and Google Docs. In addition, a vacant building was repurposed to serve as a meeting site for everyone involved in the project. This facility was situated in a relatively private area in close proximity to the main ITS offices. Evans made sure that the meeting facility was able to function as a "war room" from day one, with all requisite technology, whiteboards, and a never-ending supply of refreshments.

During the first meeting of the team leaders, Evans briefed the group on the significance of the mission. She also made it clear that this project would be her top priority and that she would be personally involved from beginning to end. She also highlighted some of the key challenges and risks inherent to a project like this one, including what might happen if the security compromise became public, scheduling conflicts with UVA programs and events, potential technical or human resource issues, system documentation shortcomings, and so on. Although all of the team leaders had a high level of experience and were willing to cooperate, it soon became apparent that there were varying degrees of what cooperation meant. In those special cases, Evans acted swiftly to make the necessary personnel adjustments.

Leveraging both Evans's support and her many years of experience managing major IT projects, German focused the group's attention to how the project would be managed. To have a shot at a successful outcome,

the team leaders would need to operate as a "team of teams,"[9] operating from a well-orchestrated plan and schedule, but with the agility necessary to respond quickly as new information emerged. German commented:

> Having managed large and complex projects in the past, I knew that the first thing we needed to do was create a project team structure. We then assigned team leads and started holding meetings every morning at nine o'clock.

As the meeting adjourned, Evans asked the team leaders to clear their calendars and begin organizing for what lay ahead. She also promised to provide additional project details in the next day or two. It was time for Evans and German to devise a plan to tackle this crisis. During one of their meetings, Hogan underscored the importance of their mission by citing a quote from *Apollo 13*: "Failure is not an option."

Everyone got the message.

Preparing to Go Dark

As part of the remediation process, it was deemed necessary by all involved that UVA would need to turn off its Internet connection, or go dark, for potentially several days in order to allow the rebuilt servers to come online, remove any compromised accounts, prevent the attackers from moving to other systems, and harden each of the layers in the network to prevent further damage. Clearly, going dark would have a significant impact on many stakeholders. Evans lamented:

> What does [going dark] mean? Does that mean everything's down? Does that mean the hospital's down? Figuring out the implications of cutting off the Internet for the university was quite challenging. What emergency situations might it create?

After much deliberation and in consultation with Hogan, the Omaha team, and as many UVA calendars as possible (a central UVA calendar did not exist), Evans and German set the go-dark phase for the weekend of August 14 through 16. It would be a real challenge to get all of the remediation work done in time, but the remediation efforts needed to be concluded before the start of the fall semester. The alternative of waiting until after the start of the semester meant increasing the likelihood that either the attackers or the length of the remediation when school was in full swing, would do harm to UVA. During that weekend, all systems would be brought down, rebuilt, brought back up, and tested. Contingent upon how that process went, the appropriate communication would go out to all internal and external stakeholders.

Then, with a firm end date decided, Evans and German sat down to devise a project plan to achieve that goal. What project methodology would make the most sense (plan based or agile) and what project-management best practices should they employ? What were the risks known to this project? How and when should Evans and her team communicate with stakeholders? Finally, when the project was finished, how would they know if it was a success?

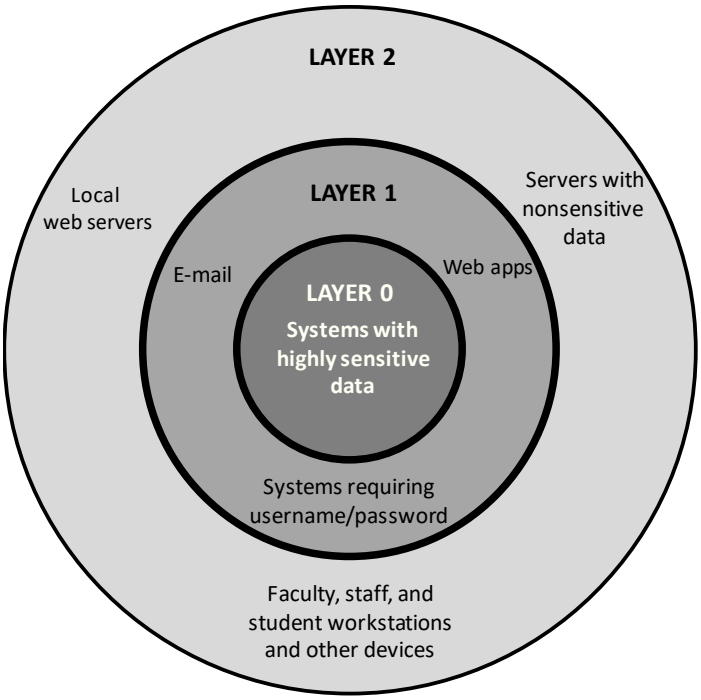
As it turned out, the next BOV meeting was scheduled for the exact same weekend as the go-dark phase. Evans was already contemplating how her next presentation to the BOV would go. Would she be reporting on a major data breach, possibly involving PII, or a successful mitigation of the attack they were now under?

[9] Stanley McChrystal, *Team of Teams: New Rules of Engagement for a Complex World* (New York: Portfolio/Penguin, 2015); the author provides a leadership framework to produce the inclusiveness and adaptability of a fast-moving start-up, at the scale of any size organization, to compete with a variety of adversaries, including terrorist networks.

Exhibit 1

The Phoenix Project:
Remediation of a Cybersecurity Crisis at the University of Virginia

Defense-in-Depth Model for IT Security



Source: All exhibits created by authors.

Exhibit 2

The Phoenix Project:
Remediation of a Cybersecurity Crisis at the University of Virginia

Organization Map