DIMINISHING *the* CYBER THREAT

A CONVERSATION WITH CYBERSECURITY LEGAL EXPERT ALLEN SATTLER REVEALS KEY STEPS COLLEGES MUST TAKE TO MINIMIZE THE IMPACT OF BREACHES.

BY MARCIA DANIEL

IN 2021, FERRILLI SIGNED ONTO PLEDGE 1%, AN INTERNATIONAL corporate philanthropy effort that encourages companies to donate 1 percent of their time, equity, or resources to support nonprofit organizations that strengthen our communities. When we first made the commitment, I expected much of our contribution to come in the form of assisting community colleges with IT modernization, cloud transformation, or business process improvements.

As is turns out, a great deal of this work has been dedicated to just one area: cybersecurity. Why? Because in Q4 2021, cyberattacks against companies and organizations reached an all-time high — and no sector experienced more of those attacks than education and research.

Ferrilli now provides 100 hours of no-cost technical consulting to any higher education institution that has been the victim of a cyber or ransomware attack — and in nearly every instance, we are seeing that the better prepared an institution is, the lesser the damage it ultimately experiences.

To that end, I recently sat down with Allen Sattler, a partner in the data privacy and cybersecurity practice at Lewis Brisbois, LLP, one of the nation's premier cyber law groups, to glean his insights on how institutions can best prepare and limit the liabilities at play. Sattler shared his thoughts on the current landscape and what every institution needs to be doing right now.

What is the state of cybersecurity in higher education today? What do the current trends portend about the frequency and intensity of future incidents?

Sattler: From my perspective, I can say that our firm responds to an enormous number of incidents — more than 2,000 on an annual basis across a number of industries. And there is a wide variety [of incidents], from the compromising of business email and wire transfer fraud to sophisticated and large scale ransomware attacks.

Over the years, we have seen a steady increase in incidents across all sectors, including higher education. The intensity or severity of each incident is trending up as well, as the tactics of the threat actors are continuously evolving. For instance, ransomware threat groups traditionally would gain access to their victims' IT environment and quickly launch ransomware to encrypt files within the network, rendering those files inaccessible and unrecoverable without a decryption key. As institutions began to strengthen their security posture, including by maintaining redundant backup and recovery systems, the threat actors evolved to intensify the severity of the attacks and place additional leverage on their victims by stealing sensitive data from their networks before launching the encryption attack, a process known in the industry as exfiltration. Higher education has not escaped this threat, and where we see evidence of encryption and ransomware, we typically also see evidence of exfiltration.

What steps should community colleges take to reduce legal liability before a cyberattack or data breach ever takes place? What does compliance look like with regard to data security today?

Sattler: Colleges and universities should be mindful of the various privacy laws and regulations in place that concern data privacy to ensure compliance, including the federal Family Education Rights and Privacy Act (FERPA). FERPA is designed to protect the privacy of student education records by addressing how and when such information can be disclosed by educational institutions covered by the law. FERPA also has certain reporting obligations that arise under specific circumstances when a covered educational institution sustains a data security incident.

It is important for colleges and universities to be aware of all privacy legislation that applies or potentially applies to them —

and it is also wise to conduct a data privacy and/or security risk assessment to determine whether their privacy policies are compliant, and to identify and remediate any vulnerabilities identified within their IT environment.

What are the most common mistakes that colleges and universities make when a cyberattack or data breach is first detected?

Sattler: It is important that colleges and universities follow their incident response plan, as that plan is usually designed for the purpose of bringing the necessary resources and parties to the table and to respond to the incident in an organized and methodical way. For instance, our firm is often engaged after a client has already taken steps to remediate by wiping impacted systems to restore and place them back into production as quickly as possible. However, that is not always the best approach, as that sometimes has the effect of deleting evidence that a digital forensics and incident response firm needs to conduct a thorough forensic investigation. Without a thorough forensic investigation, we often cannot determine the initial vector of attack to know what vulnerability in the network was exploited by the threat actor. We might also lose evidence that can show what, if any, data was exfiltrated from the network.

Incident response counsel should be engaged at the outset of any response to an incident to help ensure that the appropriate procedures are followed, to protect the privileged nature of any forensic investigation, to satisfy any reporting obligations, including to law enforcement, and to assist with internal and external communications about the incident to faculty, staff, students, and the general public.

Sticking with the topic of reporting obligations for a moment, how can colleges and universities communicate with affected parties in ways that assuage their concerns without increasing the liabilities at play?

Sattler: One of the services our practice team provides relates to internal and external communications, including, where appropriate, notification to individuals such as students and faculty whose sensitive or personal data was impacted by the incident. With regard to our clients' initial communications, we often try to give enough information about the incident to show that our client is interested in being transparent — especially with its student body and faculty. But we are careful not to disclose any privileged information, any information that is premature and not yet determined by the forensic investigation or by other means, or information that might unnecessarily induce panic.

We also provide notification letters to individuals whose personal information might have been impacted by the incident. If, for instance, the forensic investigation identifies evidence of exfiltration and we believe that individuals' personal data was compromised, it might trigger notification obligations by way of statute. Working alongside our clients, we draft the language of those letters to provide as much detail as we are able concerning the incident, including information concerning the level of risk we perceive to that individuals' data and steps the individual can take to protect themselves. Where appropriate, we also offer identity protection services, which generally include credit monitoring, access to fraud specialists, and insurance. And, in certain cases, we will open a call center for the impacted individuals to call with any questions they might have.

Besides legal and compliance assistance, what other expertise is needed for a college or university to effectively respond to an incident of data loss or theft?

Sattler: First and foremost, we recommend that our clients engage a technology partner that is familiar with their enterprise resource planning (ERP) systems and overall technology environment. We will also sometimes recommend that a public relations consultant be engaged, especially if we believe the incident might garner significant media attention. Oftentimes, the digital forensics and incident response vendor we engage to perform the forensic investigation will identify a list of files exfiltrated or otherwise placed at risk. If the vendor cannot identify a specific list of files, sometimes the vendor is able to determine the specific systems from which the exfiltrated data originated.

Depending on the amount and size of the data impacted, we sometimes engage a data mining vendor on behalf of our client to review the data and to generate a list of individuals whose personal information was contained within the data impacted. That list typically includes name and address information, as well as information related to the categories of personal or sensitive data impacted per individual.

What is the first thing a college official should do when they discover their system is compromised?

Sattler: The college should follow its incident response plan. Notifying your cyber insurer and incident response counsel are often the first steps recommended. Those teams should provide 24/7 incident response services and be ready to jump in at a moment's notice to ensure the institution has the guidance it needs in those critical early moments.

If one theme stands out to me in all of Sattler's responses, it is that those critical early moments are so much easier to navigate if an institution has done its homework ahead of time.

Do we understand what full compliance is and how it will evolve over time? Do we have a solid and practiced response plan in place? Do we know who we will need at the table should an attack ever materialize? The institutions that can answer yes to these questions may not even need 100 hours of consulting services from a firm like mine when all is said and done. If the answer is no, an institution may very well find it's going to take a lot longer than that to contain the damage.

Marcia Daniel is Ferrilli's chief client officer.