ProCircular
SECURITY. PRIVACY. TRUST.

Working with a Cybersecurity Firm for the First Time

One higher-education institution shares insights on what it's like to go through a penetration test and risk assessment

With a background in application support, St. Ambrose University's Shelly Lowery knew software and IT services – but cybersecurity wasn't part of her background.

When the university's IT director left in early 2017, however, Lowery inherited the four-person network team. And along with that role came responsibility for cybersecurity initiatives.

Before Lowery moved into her new position, the decision had been made to boost cybersecurity efforts after a conversation between the IT staff and the university's Board of Directors, which includes a few members with IT backgrounds. The Board's audit committee felt strongly about the importance of conducting a penetration test and risk assessment to evaluate network security, uncover vulnerabilities, and identify potential threats.

A cybersecurity firm had been chosen to complete a penetration test – and it was scheduled for Lowery's second week on the job. "As someone without a network background, I was panicking. I went home every night and researched terminology. I wanted to be prepared for what I heard."

To give you a first-hand look at what it's like to go through a penetration test and risk assessment, Lowery shares insights into working with a cybersecurity firm for the first time.

What a Penetration Test Offers

To check for weak points caused by improper system configuration, hardware or software flaws, operational weaknesses, or end-user behavior, ProCircular spent two days onsite at St. Ambrose University conducting a series of manual and automated techniques to evaluate network security.

The penetration test included analysis and testing of:

- Border devices (firewalls, gateways, routers, etc.)
- DMZ/network architecture designs
- Email credentials
- External IP addresses
- Internal vulnerabilities
- Onsite physical security (cameras, access control, alarm systems)
- Remote access/VPN services
- Web addresses

ProCircular SECURITY. PRIVACY. TRUST.
2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com
844-95-SECUR

Verified vulnerabilities were tested through attempts to circumvent security processes and controls. In other words, ProCircular tried to gain network access like an attacker would. If data is exposed or accessed during this testing, data retrieval is attempted to simulate how a real-life recovery attempt might play out.

As these tests progressed, periodic updates were given to the St. Ambrose team. "Amazingly enough, I didn't feel dumb sitting in the room," says Lowery. "At one point, there were three security engineers talking to me about their findings so far, how they discovered those findings, and what their impact was. I actually understood 90% of what they were saying because they were talking at my level."

Once testing was complete, St. Ambrose received a detailed technical report outlining potential vulnerabilities and reinforcing positive security measures already in place. Risk ratings were assigned to each vulnerability to help Lowery pinpoint those that needed to be the highest priority.

After analyzing the report with ProCircular and going over questions and concerns, the St. Ambrose team established priorities, strategies, and a plan of action.

Cybersecurity Vulnerabilities Revealed

Lowery wasn't necessarily surprised by what the penetration test uncovered, but the findings emphasized the importance of completing certain tasks and identified initiatives that the team needed to stop putting off.

For example, the penetration test revealed the need for a local administrator password solution (LAPS) after it uncovered a few accessible administrator accounts. To mitigate this risk, ProCircular pointed St. Ambrose to a free solution for the interim. Later on, Lowery pursued a full SIEM (security information and event management) solution.

"We had done some research on LAPS and knew we needed to do something, but we were a little nervous to pull the trigger when we didn't know much about it. During our SIEM implementation, one of ProCircular's security professionals walked our network administrator through LAPS setup quickly. Now we're confident that the issue has been addressed," Lowery explains. If a bad actor ever gains access to a password for one of these administrator accounts, access is limited to that single system.

Another vulnerability identified during the penetration test involved computers with old system images. These machines were creating vulnerabilities that could allow unauthorized access to those computers and, ultimately, to the network.

"We had been running periodic scans to find those machines, but we have some older machines just sitting in rooms. If one is shut off, a scan will never find the problem," says Lowery.

There was a simple fix to address this vulnerability as well: St. Ambrose updated all machines identified through scans as having this issue with a simple CMD line update that addressed the issue. "Approximately 30% of our machines probably had that vulnerability, and now we're down to under 5%," says Lowery. "The penetration test helped identify simple things we weren't taking the time to do."

ProCircular
SECURITY. PRIVACY. TRUST.
2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com
844-95-SECUR

The Value of a Risk Assessment

After St. Ambrose began addressing some of the highest-priority initiatives identified during the penetration test, the risk assessment began in May to uncover vulnerabilities, as well as potential internal and external threats.

ProCircular spent time onsite analyzing St. Ambrose's existing strategy documents, processes, and procedures, as well as in-house IT resources and skills.

Then, the university's existing systems, applications, hardware, and software were inventoried; potential vulnerabilities associated with third parties and vendors were also analyzed.

Once these initiatives were complete, St. Ambrose received a written assessment documenting potential threats and how likely they were to occur. Sitting down together, ProCircular and St. Ambrose walked through a customized action plan that included a roadmap and priority list to help the team confront the most important vulnerabilities first.

Lowery believes that being open to honest feedback is crucial to achieving positive results during a risk assessment. Hiding behind fear won't help you, she says. "You need to be willing to hear what you're missing and then seek advice to get the help you need. We weren't made to feel bad or that we were lacking anything, but you always worry about that. Everything was done in a very professional, thoughtful way."

For St. Ambrose, the penetration test and risk assessment went well beyond establishing security benchmarks and pinpointing opportunities for improvement – they provided a cybersecurity education and helped the team reinforce good cybersecurity habits. They also provided St. Ambrose with reassurance in knowing the right steps were being taken to improve security.

The Importance of Teamwork

Lowery emphasizes that teamwork throughout the process was crucial. With two network administrators and two assistant administrators on her team – each with their own area of expertise, including wireless and Internet access, servers, virus protection, and classroom technology – there are different schools of thought about priorities and initiatives.

Even though the vulnerabilities and fixes didn't impact everyone on the team, keeping them all in the loop provided the chance to come together and understand how each component of the network impacts something else. "It was good for everyone to see that things like one slight change to improve an area may cause problems for someone else," says Lowery. "For example, 'It's great that you secured our firewall, but you just blocked six offices from getting to the software they need.' You can't go making changes right and left without the domino effect. We've had a few situations like that – you live and learn!"

ProCircular
SECURITY. PRIVACY. TRUST.
2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com
844-95-SECUR

Looking Toward the Future

Because cybersecurity is always evolving, so are the tactics that Lowery's team uses for protection. Their next priorities include developing policies and procedures, disaster recovery, and incident response. Once these things are established, she says the university will reap the full benefits of the risk assessment.

Because St. Ambrose can't support a full-time CISO position, they also have dreams of investing vCISO (virtual CISO) services in the future. To compare possible options, Lowery has reached out to several firms to learn more about what they can offer.

"When it comes down to it, I keep going back to ProCircular," says Lowery. "Since we did the pen test and risk assessment, we've reported to the Board of Directors twice now to let them know that it was really worth the money and put us in a much better situation.

I kept telling my boss, 'They're giving us what we need and I trust them.' I can't go in with a group of people that doesn't know anything about us and try to build policies and procedures."

ProCircular
SECURITY. PRIVACY. TRUST.
2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com
844-95-SECUR