The Metropolitan
Corporate Counsel®

National Edition www.metrocorpcounsel.com

Volume 22, No. 4 © 2014 The Metropolitan Corporate Counsel, Inc. April 2014

Pay Attention: While Malicious External Cybersecurity Threats Abound, Many Others Are Hidden In Plain Sight

*The Editor interviews **Heather Bearfield,** Principal in Marcum LLP's Boston office and National Technology Assurance Services Practice Group Leader.*

Editor: Please tell us about your professional background.

Bearfield: I started my career in the IT group at a Big 4 firm where I focused mainly on financial services firms with respect to compliance and internal controls. I then transitioned to Bank of America right around the time it acquired Fleet, so there was a lot of focus on security control and such, and I was exposed to the security world to a much greater extent. From there, my boss and I moved to UHY (a predecessor of Marcum) and started the technology practice. This occurred during the Sarbanes-Oxley era, so we did a lot of internal and external controls review.

When the economy took a turn for the worse, we found many people were fearful of losing their jobs and holding data almost hostage from their company. That really kickstarted what today is Marcum's Technology Assurance and Advisory Services Practice, where we make it our mission to ensure that our clients' access controls are locked down, that their data is very much secured and that only authorized individuals are able to see and/or manipulate that data. We then put strong policies and procedures such as acknowledgment and confidentiality agreements into place. Currently I oversee our national practice, with experts in almost all of Marcum's 23 offices in the U.S., China and the Caymans.

Editor: What are some best practices around risk assessment?

Bearfield: Organizations should assess their threat level on an external and internal basis, then classify and quantify that risk, taking into account the organizational culture as well as the compensating controls the organization has in place.

Heather Bearfield

The main issue we see is that people don't take into consideration their entire risk universe. They're too close to the process, so they need to take a step back and have an independent third party come in with a fresh perspective to identify not only external threats but also, very importantly, internal threats. Identifying all relevant risks is imperative. It's critical to analyze remote access connections, the effectiveness of monitoring controls (or lack thereof) for cybersecurity threats, physical controls around the removal of data, segregations of duties, etc. For example, you may have an employee who's been with you for 30 years, and he is the only person who knows how to perform his job function. If there is no backup, and that individual doesn't have the policies and procedures written down, that's a huge risk to the organization. What would happen if he didn't come in one day? Your developer might be your sole IT person, and she has the keys to the kingdom because she can control access to the data and every aspect of the network domain. We've also seen instances where a trusted person is actually stealing from the organization: one employee developed a wire transfer application that transferred a fraction of every transaction to a different bank account.

Editor: How can these internal threats be identified ahead of time?

Bearfield: Marcum's professionals have a variety of internal threat detection tests we conduct. One service we offer that has really blossomed is a social engineering testing. In one test, we submit a phishing attack such as a happy birthday email with a link and see how many people click through. We assess the results with the organization, and they'll use the test as a training exercise for their employees. I always tell people, if you don't know the person who sent the email, don't touch the link without verifying the sender!

Another test involves sending a request to employees to reset their passwords. Invariably, the IT department reports that instead of questioning the request first, people will try to execute the process multiple times. Each step of the process – i.e., opening email, clicking the link and entering information onto the landing page – is recorded.

We also perform physical social engineering testing in which we simply observe employee behavior. For example, in one test, we tell people around the client's office that we're from the IT group and ask them if we can jump on their computer. Nine times out of 10, they don't even question us. They say, "sure, do what you need to do," then leave to get a cup of coffee. Social engineering can be especially evident in a hospital setting, where an employee might want to make a visitor feel at home and let him/her into restricted areas by holding the door – just to be considerate. Hospitals should also ensure that their wireless is separate from the guest wireless and is secure. We see too many physicians bringing in their own wireless routers to bypass stronger security measures. Think of the huge threat this creates.

Other human-error vulnerabilities include simply taking information out of the office on a USB drive and having it slip out of your pocket on the train, or emailing an unencrypted file to your personal email so that you can work on it at home. It's likely the security in your home isn't at the same standard as the organization itself! So all those instances of unprotected data are vulnerabilities to the organization.

Editor: Do you advise people to conduct employee training?

Please email the interviewee at heather.bearfield@marcumllp.com with questions about this interview.

Bearfield: Absolutely. These tests serve as a great motivator for training – no one wants to be the one who's caught creating a vulnerability for the organization. Awareness initiatives are paramount for organizations in general.

Editor: Do you see organizations protecting themselves adequately against external intrusions? Is the role of the CIO changing as a result?

Bearfield: Organizations spend thousands of dollars to make sure their financial statements are produced appropriately, accurately and timely, but few are willing to make sure they're appropriately protected from a cybersecurity standpoint. The cost of running a scan is insignificant compared to the cost of a breach, as we've recently seen with Target and others. Keep in mind a recent figure: the cost of a Social Security number on the black market has gone from $100 three years ago to a dollar or less today. One can only conclude that hackers must access entire databases of information to remain profitable.

We had a client that outsourced its intrusion detection prevention to a firm that was to send alerts everyday indicating the potential threat against the network. The client kept receiving clean reports, and, not surprisingly, it turned out the software wasn't functioning appropriately, and sure enough the client had a breach that was not detected timely. Now they're going back and conducting forensics to determine the source of the breach. No one was actively monitoring it or staying up to date on security risks.

A transformative trend we need to see continue is for forward-thinking CIOs to be extremely proactive. It used to be very difficult to breach a system, but today countless hacker websites post free codes that almost anyone could use to exploit different vulnerabilities. So IT departments have to be actively visiting those sites and staying up to date with their zero-day vulnerabilities (a hole in a software program that's unknown to the vendor) to make sure the organization is doing everything it can to protect itself.

The more technology an organization offers, the more risk it exposes itself to: with each product comes a whole new set of risks, so each must be actively monitored. CIOs and IT departments can't just rely on the technology and the monitoring controls that are already in place.

Editor: What is involved in ensuring appropriate controls and accurate reporting around risk?

Bearfield: No organization can protect itself 100 percent; you have to do what's reasonable for your organization. Classifying the types and sensitivity of your data and information that you store is the first step – again, conduct a risk assessment. Then apply those controls that are relevant to the level of risk. For example, we have many organizations where the IT department may not have complete segregation of duties. An appropriate control for them may not be hiring three extra bodies, but instead instituting compensating controls such as restricted access for certain transactions, or having audit logs or implementations reviewed. At the end of the day, organizations have to conduct their business. Working with them in depth will help them learn what is appropriate for them based on that data classification.

As for accurate reporting, we do a lot of support for financial statement audits. In the more complex organizations we'll audit through the system instead of around the system. This means that we can validate that inputs are being processed accurately, so that the export of the report is accurate, appropriate and completed in a timely manner. We make sure that the users of each of these applications have been restricted based on their job responsibilities.

Editor: What are the best first steps when a breach (or worse) happens?

Bearfield: It surprises me to this day how many organizations don't have a solid disaster recovery group or business continuity plan in place, even after 9/11 and the many natural disasters we've seen.

First and foremost, you need to know how you're going to keep your systems up and running. Make sure that you have reliable and recoverable backups, that you have a hot or a cold site from which you can bring your operation back up and functioning again. Make sure you can execute the plan when the time comes. A lot of people perform backups of their information but they never make sure they can recover it.

From a business continuity plan (BCP) perspective, many people today are leveraging social media so that when a natural disaster hits, people can still contact each other. This can be very helpful as a secondary measure, but if social media is going to be the primary source of information, this should be incorporated into the BCP plan itself immediately and communicated out so people know to go there and look for information and broadcast updates. We've unfortunately seen time and time again that it is absolutely necessary to have an executable, locked down concrete plan.

We've also seen – even with our own clients – cases where hackers have locked down one of the servers and literally held it hostage for ransom. Obviously, if you don't have a solid backup solution, you're going to end up paying. Fortunately, in every one of our clients' instances, they had a solid backup plan in place and were able to recover that information without having to pay.

Editor: How can individuals protect themselves?

Bearfield: We've been conducting a lot of presentations on this topic. First, be careful what you post on social media. As you likely know, employers are increasingly using social media to screen potential employees. But displaying information about yourself on these sites presents another problem from a security perspective. Many low-level hackers can guess your username, and your password can often be reset by use of security questions. Answers to many of these security questions can be easily found on your Facebook or LinkedIn page if you're not careful. So making those security questions very obscure is becoming increasingly important. There's a trend toward more complex security questions, and in some cases you're given the option to actually write your own. Individuals really need to be smart about the information they're sharing and using strong passwords.

Editor: You were recently quoted in a *Wall Street Journal* article about internal threats, some of which we've discussed. Any final words of wisdom for organizations?

Bearfield: People need to be more aware of internal threats. We worked with an organization that had a breach, and after conducting an external assessment, we discovered they actually were locked down from an external perspective. But then we conducted an internal assessment and found they were wide open. People were storing their passwords underneath their keyboards or on their bulletin boards, etc. This really gave everyone access to basically everything. It was like the Wild West. In fact, the person whose computer caused the breach wasn't even at work that day, and his password was right underneath his keyboard. Since user names are easily guessable, make sure you have strong password policies in place and train your employees regarding strong security practices.

It's critical to raise awareness. Many times organizations tell us everything's working fine, but when we run a scan, we find all kinds of threats. Until it hits home, people don't understand how vulnerable they actually are.