Compliance & Ethics Professional®

April
2016

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org

Meet Mark Lanterman

Chief Technology Officer
Computer Forensic Services
Minnetonka, MN

See page 14

Mark Lanterman
Chief Technology Officer
Computer Forensic Services
Minnetonka, MN

an interview by Adam Turteltaub

Meet Mark Lanterman

Mark Lanterman (mlanterman@compforensics.com) was interviewed in January of 2016 by **Adam Turteltaub** (adam.turteltaub@corporatecompliance.org) VP Membership Development at SCCE/HCCA.

AT: Cybersecurity is a bit of a nightmare issue. We just did a survey among compliance professionals, and they named it one of their top areas of concern for 2016. It's not surprising, given the headlines. I also well remember a couple of years ago at the Compliance and Ethics Institute when the Director of the FBI gave a scary talk on the topic. Is the risk getting greater or smaller?

ML: That's a good question. The best answer I can give is this—it's all proportional. By that I mean, the threats are no doubt growing in size and scope. As we come to rely more and more on technology, the bad guys are seeing more and more potential to steal and line their own pockets. By its nature, cyber threat intelligence is always a step behind the bad guys. Therefore, the risk is definitely one that is growing and will persist well into the future. Luckily, though, awareness and the market for digital security are also growing.

AT: One of the things that I find most troubling about this issue is that there are so many potential intruders. You could have a hacker wanting to access your system for fun or malicious reasons, state actors and competitors looking for trade secrets, and let's not forget employees with a grudge or who are just careless. How would you prioritize the risks among these and other potential sources of breach?

ML: Motive is important in analyzing and understanding cyber breaches in order to prevent them. However, I don't think it should matter what a hacker's motive may be. Every breach should be treated as a malicious, serious, and potentially damaging threat. That said, the nature of different threats, and consequently, the potential damage of a breach, is really dependent on an organization's digital infrastructure. Thus, organizations are really in the best position to rank these threats for themselves. We have certainly seen that different organizations are in different spots on the spectrum.

AT: Are there specific strategies that companies should employ to counter each of these threats? If so, what would they be?

ML: While there are specific measures that organizations can take, it is highly dependent upon the variables in a given organization. In other words, there is no "one size fits all" for a strong digital security plan. Furthermore, the technology changes on a daily basis. The most secure companies are the ones that do not let their security plans grow stagnant. The best are those that account for changes in the technology, educate employees, and audit consistently.

AT: What do the strategies all have in common? Put another way, what should every company be doing right now?

ML: Our primary observation over the years has been that data breaches occur because of a simple lapse of judgement. The single most important aspect of security is people. The human element of technology is just as, if not more, important than the tech itself. It can only ever be achieved through education and strong implementation of written digital use policy. I like to refer to this as fostering a "culture of security." Therefore, I think that companies should be educating their employees on a regular basis about the realities of digital attacks, how to recognize them, and what to do in the case that something does happen. Such education programs should cover everything within the company's digital security policies—from mobile devices, to social media, to passwords and encryption and backups.

> Our primary observation over the years has been that data breaches occur because of a simple lapse of judgement. The single most important aspect of security is people.

AT: What are some of the common mistakes you see companies making when it comes to shoring up their cyber defenses?

ML: I think the biggest mistake I have seen is over-confidence. Many organizations believe that they have done all they can to prevent a breach, and are thus absolved from putting in place any sort of contingency plan should a breach occur. These organizations adopt a posture of: "Something like that cannot possibly happen to me." When breaches happen, too often the C-suite executives are caught looking like deer in the headlights. As the old adage goes, "Hope for the best, but prepare for the worst." Therefore, I recommend that an organization take the time to delegate roles and responsibilities and have a plan of action should its worst fears be realized.

AT: Compliance officers are increasingly getting involved, if not taking charge, of this aspect of IT. What's the first thing a compliance officer should look for when assessing the risk of cyber attacks, and their company's defenses?

ML: Compliance officers have an interdisciplinary job. They need to educate themselves not only about how the different technologies within their organization's network, but more importantly, they need to understand how those technologies are being used. I advise compliance officers to remember one key fact: No hacker (unless you have been breached already) knows more about your organizations digital infrastructure than you. Compliance officers have the potential to learn everything there is to know about an organization's digital and non-digital assets. I recommend that compliance folks take the time to not only learn the tech, but also use their discretion to prioritize which assets need the most protection.

> I advise compliance officers to remember one key fact: No hacker (unless you have been breached already) knows more about your organizations digital infrastructure than you.

AT: How much does a compliance officer need to "get into the weeds" of security protocols and other technical factors? Is it time to get some training, or best to leave the technology decisions to the experts?

ML: In order to effectively manage and audit digital security, compliance officers should absolutely have a general understanding of the technology to a point where they would feel comfortable with the jargon between Legal and IT in the event of a breach. It is important to know about what happened in order to report it and prevent it moving forward. As far as "getting into the weeds" or minutiae of the technologies, I don't think that is necessary. I think the best compliance officers know that when it comes to digital security, outside vendors and digital security contacts are absolutely necessary in most cases, no matter how many details a compliance officer knows about the tech.

AT: You do a lot of computer forensic work, which leads to another area of cybersecurity: making sure you aren't holding onto documents longer than you should. Are companies getting better about their document retention practices? Or do they still have policies and haven't gotten to the real putting-them-into-practice stage?

ML: That is an excellent point. Document retention practices are actually a key aspect of digital security. Keep too much for too long, and you have that much more information that can potentially fall into the wrong hands. Keep too little, and there may be serious inconvenience factors, costs, and other issues. A good security plan always accounts for the volume and type of data that is available. More importantly, it also addresses where the most important digital assets are located, so that the proper resources can be diverted to an organization's "crown jewels." But this question is really dependent on the policy choices an organization and, perhaps in some cases, what an industry's standard dictates.

AT: I remember a few years ago there was a lot of press about companies getting rid of old photocopiers and not realizing that thousands of their documents might be stored on them. I imagine most have gotten better about that, but should compliance officers be worried about all the old laptops and smartphones hanging around? Are they being disposed of properly?

ML: As much as the industry should be concerned about external attacks, it is important to not forget about the smaller, seemingly innocuous security lapses. Data exfiltration from negligence happens all the time, which is a shame, given how easy it is to prevent. Think about a breach in the form physical device theft. For instance, as you know in the healthcare industry, data breaches that affect 500 patients or more must be reported to the U.S. Department of Health. Hundreds of reported incidents involve stolen laptops and phones. With theft, there is clear evidence that data has been stolen. In the case of disposal, companies often fail to securely wipe data before selling or recycling. Failing to recognize this, these types of breaches would never be reported, as no one would expect anything to be wrong.

AT: That leads to one last area to explore: smartphones. These days most everything is kept on them. How secure are they? What should compliance officers be asking their IT teams to make sure that they truly are secure?

ML: Mobile devices have changed how work gets done. While they are often secure, it all depends on how they are used. There are always threats that are unique to mobile computing. For example, like public restrooms, public Wi-Fi should never be trusted like your own. Public Wi-Fi networks are very useful, but there is always a risk in using them, because they can be a portal for cyber criminals to steal your valuable data, including usernames and passwords. This alarming trend is what is known as a "man-in-the-middle" attack. Essentially, this kind of attack enables a hacker to eavesdrop on your Internet connection, intercept your communications, and in some cases, reroute your connections to their own malicious webservers and material. For many websites you may visit regularly, a hacker can remove the encryption from the websites' secure login pages. Again, there is always the persistent and very real increased risk of device theft, not just of smartphones, but all mobile devices. Considering all this, I would suggest that compliance officers ask IT about public Wi-Fi use prevention and data encryption. With encryption, data on mobile devices is rendered inaccessible to a thief.

There are always threats that are unique to mobile computing. For example, like public restrooms, public Wi-Fi should never be trusted like your own.

AT: So, once the company-issued devices are covered, that's only halfway there. There are still the personal devices that employees are using. What protocols should be in place if a company has a "bring-your-own-device" policy?

ML: Unfortunately, in most instances, bring-your-own-device (BYOD) relinquishes some defined, universal security strategy, and inherently gives an organization less in the way of data control, because standard mobile device management tools are not used with employee's personal devices. Many smartphones also offer device tethering, whereby the phone's cellular data connection is shared with other devices. This type of network activity is not monitored. Before simply accepting BYOD as a cost effective and desired approach, ensure that policy is clear and consequences are clearer. Also consider with Legal whether there are special regulatory concerns particular to a certain industry. In some industries, like healthcare for example, such a lack opens up serious liability.

Beyond BYOD, I also urge compliance professionals think about BYOC (bring your own Cloud). The risk with BYOC is two-fold. First, it can be an avenue for disgruntled employees to easily take information with them after leaving. Second, they also pose unique mobile security risks. Interestingly, rather than stealing a username and password, cybercriminals have found a way to steal and use password "tokens" that are stored with a Cloud application on a user's mobile device. These tokens store a user's credentials for convenient access from a trusted device, making it so a user does not have to re-enter a username and password each time they access the app. By using other types of attacks, such as Wi-Fi exploits or a phishing attack, this credential token can be stolen and used to authenticate another untrusted device. Since this token is unique to a legitimate "login" session, it makes detection difficult, and even the service providers will have a hard time detecting the compromise.

AT: Finally, given the threats out there, is it time to start asking a very hard question: Should some of our data NOT be available through our network? Is there some data that's safer if we keep it offline on a desk somewhere?

ML: That is a very hard question and not one I can answer for everyone. It is all about finding that magic recipe that balances convenience with security. It is important to remember that there is no such thing as perfect security, no matter where or how data is stored (whether digitally or on paper). Just because it's not connected to a network does not mean it cannot be stolen. In many ways, storing information digitally allows for greater control of access privileges.

AT: Thank you, Mark for sharing your insights with us.✳

Compliance & Ethics Professional
April 2016
A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS
www.corporatecompliance.org
Meet Mark Lanterman
Chief Technology Officer
Computer Forensic Services
Minnetonka, MN
See page 14
29 EU Data Protection Regulation: Are we nearly there yet? Jonathan P. Armstrong
33 Marketing and Data Security Practices: The FTC v. LifeLock settlement Keith M. Gerver and Peter T. Carey
39 "To disclose, or not to disclose? That is often a tough question." Peter Anderson
45 The Ethics Wheel: Shaping corporate culture Susan Korbal