Addressing Insider Threats, Cyber Attacks & Data Security

Insider Threats

When we talk insiders, we have to start with the basics, because whether we like or not that this the state of the industry right now. As a group we have focused on layered protection at the perimeter. The specter of evil, thieving hackers and the headlines have produced a reaction that as a whole ignores the more potent threat to an individual credit union – the insider.

Insiders threats, malicious and inadvertent, represent 55% of the breach activity for last year (IBM 2015 Cyber Security Intelligence Index). 55%. Is 55% of our attention and budget placed on that threat? The answer for most is a resounding "No."

The first step is education. Educate management and the board as to the threat, make it real and relevant. Then resources will follow, but education is the single best protection a bank can have and it can never stop. If/when resources allow, we deploy a product that enables us to arm the client with what is an intelligent "Big Brother" set of information. The IT resource belongs to the client and they are entitled to use baked in intelligence to highlight a pattern of suspicious activity and focus on an employee who may be going south. We enable that management and find frequently just knowing someone is watching makes employees (1) more security conscious in their client interactions (2) more self-aware about their personal onsite activity.

The second step is threat intelligence. It is vital that limited security resources be focused on relevant outside threats. We enable that through software that hones in on only the systems that the bank and its vendors use. By focusing the security department on what may be imminent our client's in house staff is better utilized. We of course stand in the ready to assist and escalate when a potential threat becomes real.

Breach

It is 2016. Breach is real. What is worse is that the top of the target list is the small to medium sized financial institution because, the bad guys correctly assume, they represent a softer target than the large financial institution.
Breach is also inevitable. The financial industry is coming to understand that you can't buy security and eliminate risk, but only consume security and reduce risk. With that realization comes the responsibility to prepare for breach in the same way that 911 convinced us to start building BCP and DR plans. 2016 will be a year where the industry continues to explore what it is like to prepare and how to survive a breach.

Emergent Threat

In the upcoming year, we see more probing of mobile. Mobile payments and other financial software is still in the wild, wild west days in its maturity. But, the phone is ubiquitous. The client is enrolling in mobile banking and payments systems with a voracious appetite and until we have a better system of tokenization, there can be great reward from this vector. We advise vigilance in this area in particular.

Data and File Security

Our advice in this area starts in the same way as it does when we talk insider threats – education. First, the financial institution needs to know where their valuable data is, specifically personally identifiable information and account information. We then protect it in the following ways:

1. Encrypt at Rest.
2. Encrypt in Transit including on private networks like MPLS.
3. Use SIEM to correlate network activity that is suspicious especially if it is new or directed at a vital storage location.
4. Control Passwords.
5. Work Fast.

The last bullets always get attention. In relation to passwords, their complexity is the Achilles heel. Single Sign-on is great, but can be a challenge. It just isn't ripe yet for many organizations. So we offer easy to use two-factor authentication password management that allows the employees' passwords to be managed (frequently they don't even see the password).

Work Fast. We are very aware that once breached data leaves at lightning speed. Many hacks are only evidences while the hacker is actually on the client system and then is hidden while they aren't active, and can go on for months. So we are constantly tuning our systems, human and otherwise, to work fast when/if malicious activity is evident. The hacker extracts value in minutes, sells it in hours and we can't be late to that table. Working fast and then faster still is key to protecting data.

Mark Berman
Co-Founder and Principal

Horsetail Tech

Contact Info
www.HorsetailTech.com
410.560.5601

Mark Berman is a Principal and Co-Founder of Horsetail Technologies, LLC. He graduated from The College of William and Mary with a degree in Computer Science and from Loyola University with a Master's in Business Administration. Berman has a variety of Cisco and Dell Security certifications and is active in the compliance area of financial institutions. The Horsetail Technologies Managed Service Program (MSP) was developed to provide your bank with the technology services that you need so that you can focus on your business. Our state of the art systems and experienced staff allow us to offer a wide variety of customized programs that fit your needs.