

Meeting the Challenges of Attacks, Breaches & Compliance

Take a Dose of Reality add Two of Preparation and Call me in the Morning

Breaches will occur. That is the reality of 2015. Every credit union should expect and prepare for a breach and prepare for the aftermath. The days of “if” are gone and the days of “when” have arrived. To those of us in the business of providing security, people who watch read reports almost daily of successful attacks, it may seem like obvious advice, but there are a tremendous number of CEO’s who still are believing that they may escape without being the object of an attack. For every two of those there is another sitting in a cocoon believing otherwise and dealing with aftermath of a breach or an attack.

So before we talk about tools and services, strategies and tactics. Be honest. Be real. And get all the stakeholders on the same page.

The next dose of reality is that we can employ the best tools that the industry has to offer, and it still won’t be enough. Whether it is the AC repairman that taps into Target’s network, or tools that are purchased, but unknowingly not perfectly configured, we need to use tools like SIEM programs and, yes, human resources who can recognize unusual traffic, information flow patterns and atypical user behavior to identify the breaches that make it through the gaps.

It may sound obvious, but this does not mean that we don’t deploy the best tools available. We do. The object is to make the gaps as small as possible for the SIEM systems and their caretakers to be as focused as possible on genuine threats.

The Relevance of the Regulator

We love to complain about the NCUA and their state counterparts. The reality is that regulation is always a lag behind the evolution of an industry and is by default – reactionary. In the case of the challenge of the threat landscape, the regulations should be used as an insufficient minimum standard – and nothing more. Anyone who has sat through a number of examinations learns quickly that the IT professional knows more than the examiner in most cases, and if you are missing the mark on an exam, then there is real trouble and immediate correction is warranted. If you need to know what is in the exam, you can establish a trial account on AiresLive.com, go to the security sections and see for yourself exactly what the examiners are looking for.

Waiting for the Call

If you have deployed the Anti-Virus, Anti-Malware, firewalls, encryption at rest, encryption in motion, portable device blocking, SIEM services, locked down desktops, content filtering, regular report reviews, most importantly instituted regular training and all of the other basic tools to secure the CU network, it is time to deal with the reality by doing the same thing – prepare. The credit union can and should buy proper insurance to cover the costs of a breach. Making executives aware of so-called “Cyber Insurance” is also part of the job of IT. Additionally, CU marketing and public relations departments can prepare for a breach and practice procedures in the same way that DR is planned and practiced. The reality is that breach and hacking preparation has a much higher probability of occurrence than an earthquake, so prepare and deploy resources accordingly. Then, sit back and wait, of course hope that it is never used, but be ready to recognize and respond if an attack or breach happens.



Mark Berman
Co-Founder and Principal



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 the credit union movement. The Horsetail Technologies Managed Service Program (MSP) was developed to provide your CU 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.