XM CYBER

WHY IT SECURITY FAILS

By Richard Benigno, SVP Global Sales, XM Cyber

Here's the unvarnished truth about IT security: Even if you stack product on top of product and schedule regular user training, even the most robust security defenses can be undone by a simple user error. Even more maddeningly, these mistakes often seem absurdly foolish in retrospect.

Yet while sloppy IT practices might make it easy to point the finger at some hapless user who fell for a routine phishing attempt, that viewpoint misses the larger picture. We can call out our colleagues all we want, but humans are simply hardwired to be susceptible to an IT security fail.

THE ROLE OF HUMAN NATURE IN IT SECURITY ATTACKS

To understand why humans are the weak link in IT security, we need to consider how we think. Research has shown that the human brain has a tendency to create heuristics, which act as "decision-making shortcuts" that allow us to conserve mental bandwidth when confronted with uncertainty. Heuristics allow us to make a decision perceived as "good enough," while conserving our effort for other tasks. Heuristics are one reason why humans are quick and efficient in terms of cognition -- an evolutionary advantage that helped keep our ancestors alive when confronted with larger and faster competitors.

Yet this same tendency can work against us. In modern society, we are inundated with messages competing for our time. We are easily distracted and lulled into making suboptimal decisions. These messages are also often designed to appeal to our brain's reward system. If a phisher dangles a free prize or some other inducement, our brains may register concerns, but those concerns may be quickly overridden by the prospect of receiving something we desire. In a world where the demands on our attention are greater than ever -- and we've been conditioned to keep clicking in order to receive another jolt of dopamine -- it's hardly surprising that some people fall prey to phishing attempts that seem silly in retrospect.

Yet while human nature may be the most significant role in cyber security fails, it's not the sole reason why incidents occur. Let's take a closer look at a few, more technical examples of common failure points.

AVOIDING INDUSTRY STANDARDS OR NOT VETTING SECURITY PARTNERS

While "security by obscurity" may offer some value, it's often outweighed by the vulnerabilities associated with taking a non-standard approach. Opting for an industry standard means that the algorithm or approach you're using has been rigorously vetted by experts. Standards are also subject to continuous analysis and review. If one standard isn't up to par, new standards can be developed.

This isn't an ironclad rule, of course, as proprietary tools can play a critical role in your overall security posture. It's important, however, to work with partners who can back up their claims.

MISDIAGNOSIS OF ISSUES

You can have the best security products in the world, but if you haven't clearly defined the problems you're attacking, it may not matter. A great solution that doesn't address your real vulnerabilities may leave you critically exposed.

One simple example: A firewall might offer robust protection in some ways, but little-to-no protection in other contexts. Without a dedicated solution to all relevant issues, security gaps can leave your "crown jewels" exposed.

FAILING TO PRACTICE SMART SAFETY PROTOCALS DURING CLOUD MIGRATION

While the previous examples are somewhat evergreen to IT, here's one that is especially relevant today. As companies rush through cloud migration, they often put unrealistic demands on their overstretched security teams.

They also fail to consider the specific challenges inherent to security in a hybrid environment. Security teams need to consider on prem security objectives, cloud security objectives and -- most importantly -- the interplay between on prem and cloud. This is illustrated by the stream of major cloud security incidents we've seen lately, often arising from a simple misconfig or some other seemingly obvious security flaw. AWS and other cloud environments are also at elevated risk of attacks from advanced persistent threats (APTs), who can embed within networks and move laterally, escaping detection for weeks or months.

Other common IT security fails include:

- Implementation of standard IT networks into operational networks
- Poor IT hygiene (changing permissions and forgetting to switch them back)
- Vulnerabilities related to data maintained on third party supplier/customer networks
- Improper connection and USB errors that can jeopardize even air-gapped networks

SO WHAT'S THE SOLUTION?

As noted above, human nature is the ultimate security vulnerability. You can have the most advanced vulnerability scanners, penetration testing, patch management tools etc., but you still need to account for how people are hardwired to think.

Given that IT security fails are inevitable, it's imperative to use the most rigorous and continuous testing tools available. For APT IT security, breach and attack simulations (BAS) fit that description quite well.

A relatively new technology, BAS platforms simulate the most likely attack paths taken by APTs and expose these gaps. In this way, BAS platforms act much like red teams, ethical hackers who help launch attacks in controlled environments in order to test defenses. Once issues are exposed, prioritized recommendations are issued.

There is one critical difference between BAS and red teaming, however: Advanced BAS platforms offer automated testing. Instead of relying on pen testing every few weeks, organizations can assess the state of their security 24/7, 365 days-per-year.

Currently, this level of automation provides the gold standard in APT IT security, as it effectively addresses all the modern IT failure points outlined above through automation and continuous testing.

THE TAKEAWAY

Like death and taxes, IT security fails will always be with us. Yet by accounting for human nature -- and using cutting-edge solutions such as BAS platforms -- organizations can greatly reduce their risk of becoming the next high-profile IT security fail.

Research has shown that the human brain has a tendency to create heuristics, which act as "decision-making shortcuts" that allow us to conserve mental bandwidth when confronted with uncertainty. Heuristics allow us to make a decision perceived as "good enough," while conserving our effort for other tasks.

ABOUT XM CYBER

XM Cyber was founded by security executives from the elite Israeli intelligence sector.

XM Cyber's core team is comprised of highly skilled and experienced veterans from the Israeli Intelligence with expertise in both offensive and defensive cyber security.

XM Cyber has developed more than 15 patented technologies based on a proprietary set of algorithms that enable the continuous and automatic simulation of a hacker's techniques and methods.

RICHARD BENIGNO

Richard Benigno is Senior Vice President of Global Sales at XM Cyber. He has more than 20 years of experience working with enterprise security organizations, helping CISOs and security leaders with their strategic initiatives around the globe. He has held executive positions at leading security vendor companies, including CA, Stonesoft, Intel Security, Tenable and Insights Cyber Intelligence.

XM CYBER®

Tel Aviv +972 3 978 6668 New York +1 866 598 6170 London +44 203 322 3031 info@xmcyber.com