Is a Hollywood hack just around the corner? Can malware attacks get any meaner? Will there be any good news in 2014? Read about tomorrow’s security headlines today in WatchGuard’s 2014 Security Predictions. The insights you gain can help you prepare your defenses in advance, for a safe and prosperous year of business.

EXPECT A HOLLYWOOD HACK IN 2014
A major state-sponsored attack shows us infrastructure hacks don’t only happen at the cinema

You’ve seen it in the movies. A big hack that drains the Federal Reserve Bank, shuts down power in all the big cities, or causes a critical dam to fail and flood the town downstream.

These types of cyber attacks sound like science fiction. However, our critical infrastructure really does rely on computers and – despite best practices saying otherwise – we are slowly putting some of this infrastructure online. Even if we keep these systems air-gapped (offline), the often-cited Stuxnet proved that motivated cyber attackers can infect non-networked critical infrastructure, with potentially disastrous results.

As a result, researchers have spent the past few years discovering and studying the vulnerabilities in industrial control systems (ICS) and supervisory control and data acquisition (SCADA) solutions, and their findings aren’t comforting. These systems have many holes.

We think a malicious actor or nation-state will realize a Hollywood-like hack next year, by exploiting a flaw against critical infrastructure.

INCREASED CYBER KIDNAPPING RAISE ATTACKER PROFITS
Hackers concentrate on ransomware to steal more money

Ransomware is a class of malicious software that tries to take your computer hostage. It “kidnaps” your important files, making it so you can’t access data or use your computer. Criminals then try to extort money to regain access.

A particularly nasty variant, Cryptolocker, emerged in 2013. It arrives in various ways, including as a phishing email attachment, or through websites hosting malicious drive-by downloads. It encrypts many of your important files, including Office documents, pictures, and digital certifications. Then it demands $300 to get them back.

Cryptolocker uses industry-standard encryption to ensure you can’t reclaim your files. It uses domain generation algorithms (DGA) to make sure it can always reach its master, and it uses Bitcoin to make it harder for authorities to track these illegal payments. Cryptolocker has affected millions and we suspect its authors got a sizable return on their criminal investment.

Modern cyber criminals are not stupid. They pay attention to others’ success, and look for ways to increase their ROI. In 2014, you can expect cyber criminals to try to copy Cryptolocker’s success by mimicking its techniques and capabilities. Plan for a surge of ransomware in 2014.
HACKERS HARASS U.S. HEALTHCARE HANGOUT
The US HealthCare.gov site will suffer a data breach

In the United States, the new Affordable Care Act, colloquially known as Obamacare, hinges on the use of online healthcare insurance exchanges, where patients can purchase healthcare at discounted group rates. Here are two main reasons why it is such an attractive target.

First, as the online cornerstone of the new US healthcare system, Healthcare.gov will certainly garner a lot of attention. Imagine you’re a hacktivist trying to make a big political statement... what better place to capture the notice of millions?

Second, in order to do its job the site needs to ask citizens for personally identifying information (PII). This makes Healthcare.gov, and all the online exchanges under it, an important overseer of sensitive data, which obviously makes an alluring target.

We believe both good and bad hackers will take aim at Healthcare.gov in 2014. In fact, it’s already happened to some extent. We’ve seen evidence of attempted (unsuccessful) web applications attacks, and attackers have tried to DDoS the site.

None of this is to say you should avoid Healthcare.gov, or that it’s any worse than any of the millions of other websites we share our valuable data with. In fact, its current high profile means that the folks managing it will focus heavily on its defense. We’d argue that in time, Healthcare.gov will likely be more secure than the majority of sites out there. However, we also know things sometimes have to get a bit worse before they get better. That’s why we forecast that Healthcare.gov will suffer at least one data breach in 2014.

NETWORK ATTACKERS BECOME CYBER SHRINKS
Criminal attackers will up their social engineering game in 2014

The information security battle has always been a pendulum, with the technical advantage swinging back and forth between attacker and defender. As defenders develop new security technologies to get a leg up, attackers develop new evasion techniques and reclaim advantage. The cycle goes on ad infinitum.

The last few years, attackers have had the advantage, leveraging highly sophisticated attack techniques and using advanced evasion tactics to get past legacy defenses. Now the tide is turning. Next year, defenders will have more access to new advanced threat protection capabilities and next-generation security solutions, swinging the technological security pendulum back in our direction.

While that’s good news, don’t expect cyber criminals to give up that easily; rather expect them to change their strategy.

There are two ways attackers can compromise our networks. They can exploit technical weaknesses or they can prey on sociological ones. As we regain the advantage, expect cyber criminals to refine their social engineering skills, and concentrate more on attacking flaws in human nature. In fact, they’ve already done a good job in this area. Their phishing emails are better written and more convincing, they’re masters at leveraging pop culture, and they know our worst habits.

In 2014, you should expect attackers to focus more on psychology than technology, and target your weakest link—the user. Spend some time investing in user security awareness training to protect yourself from next year’s cyber threats.
HIGH-PROFILE TARGET SUFFERS A CHAIN-OF-TRUST HACK
Hackers infiltrate a big-name victim through its smaller partners

Cyber attackers have clearly gotten more sophisticated over the years, especially those associated with state-sponsored hacking. These advanced hackers target a higher level of victim, regularly going after government and military organizations, critical infrastructure providers, and Fortune 500 businesses.

Top-level victims tend to have a higher security pedigree, and do NOT pose soft targets. Yet, they still can fall to the persistent, advanced attacker who preys on the weakest link in a victim’s chain of trust - their partners and contractors.

In many of the most sophisticated attacks, bad actors first had to infiltrate secondary or tertiary targets in order to gain access to some asset needed to compromise the intended victim. For instance, hackers targeting Lockheed Martin first had to steal SecureID seed data from RSA (their ultimate target may have been the US military, a customer of Lockheed Martin). We’re also seeing more and more cases where attackers hijack digital certificate providers, or steal the certificates from smaller companies, for use in a more specific targeted attack.

As advanced attackers go after harder targets, we expect to see more “chain-of-trust” cyber breaches, where hackers hijack your partners in order to gain access to your organization. Expect at least one headline-grabbing chain-of-trust breach next year.

MALWARE GETS MEANER
Expect an increase in destructive viruses, worms, and trojans

Security professionals often like to imagine worst-case scenarios. You know... like some doomsday malware that deletes everyone’s hard drives, launches the world’s complete arsenal of nuclear weapons, and evolves into an evil, self-aware “Skynet” to enslave humankind.

While entertaining to imagine, and sometimes even theoretically possible, these worst-case scenarios are rarely seen in the real world. Most cyber attacks and malware are not purposely destructive. If you think about it from the attacker’s perspective, it just doesn’t make sense to destroy your victim’s resources. If you destroy their computers, you can’t spy on them and gain access to other resources. Not to mention, you also give yourself away.

Cyber destruction, however, may well become a valid goal for 2014’s network attackers. For example, hacktivists or nation-states actors who want to send a brash message or disable an adversary’s systems may turn to destructive attacks, like the case of the disk wiper malware seen in a South Korean attack. Cyber criminals may also realize the threat of imminent destruction could help increase cyber extortion success rates.

Whatever the reason, we think malware will get meaner in 2014, and you can expect to see more cases of destructive malware and attacks.

BAD GUYS BREAK THE INTERNET OF THINGS
White and black hat hackers spend more time cracking non-traditional computer devices

There are computers in everything! Ok... not literally, but we do have them in cars, pace makers, televisions, watches, kids’ toys, cameras, baby monitors, and we are even trying to strap them to our head inside a pair of eyeglasses. Furthermore, most of these non-traditional computers include all kinds of interesting, information-gathering sensors, including GPS, accelerometers, altimeters, photodetectors, and good old fashion cameras (video and still). Finally, most of them can connect wirelessly, and they treat security like an afterthought.
When you add this all up, it’s like Christmas for hackers. The Internet of Things (IoT) provides a playground of connected devices for curious or malicious computer experts to have fun with. Want to make a car think it’s flying? You can! How about trolling a baby over the Internet? It’s been done. However, things can also take a dark turn as well, with an ex-vice president disabling his implanted defibrillator’s wireless feature to avoid assassination.

Security experts have warned about securing the IoT for a while now. However, the market is just now catching up with the expectation, with more and more embedded computing devices showing up in stores every day. We suspect good and bad hackers will focus heavily on finding holes in these non-obvious computing devices this year.

2014 IS THE YEAR OF SECURITY VISIBILITY
_INFOSec Pros realize you can’t protect what you don’t see_

Cyber attackers have successfully breached some very big companies, despite the victims having many security defenses, including firewalls and antivirus. Furthermore, many of these victims didn’t even realize they were compromised until it was much too late.

So what’s the problem? Do our cyber security controls not work or are we doing something wrong?

We think the issue is threefold:

a. **Most businesses still rely on legacy defenses**, such as stateful packet filtering firewalls, which don’t help against today’s threats.

b. **They don’t configure their security controls properly**, and often don’t enable their best defenses, or accidentally bypass them. (In fact, Gartner says 95% of firewall breaches are due to misconfigurations).

c. **They are drowning in oceans of security logs**, making it impossible for them to recognize the important security events that they need to react to.

This year, CSOs and security-focused IT managers will tackle these problems, and focus more on deploying security visibility tools, which can help them quickly identify security-related issues in their organization. These tools highlight the most important security and business trends in the network, and in turn, this analysis can guide them toward making proper security and business policies to better protect their companies. Expect 2014 to be “The Year of Security Visibility.”

**Conclusion**

Naturally, network security predictions are going to be rife with worrisome attack scenarios and escalating danger. But note that in our 2014 predictions, there is reason to be optimistic. Being diligent in educating your users on smart security habits and taking steps to upgrade to the latest defenses will pay off for savvy IT professionals. The best news of 2014 underscores the truth of that old saying, “Visibility is security.” If you can’t see what’s happening in your network, how can you possibly defend it? New visibility tools are making it possible to distill oceans of security data into actionable security intelligence and that’s where businesses can gain an edge over cyber criminals. We encourage you to make 2014 “The Year of Security Visibility” in your business network.

**WatchGuard Technologies** provides an extensive family of network security products to help you secure your network from advanced attacks, prevent drive-by downloads, layer best-of-breed defenses, and much more – all with unprecedented visibility into network security activity. For more information, contact your reseller or visit us at [www.watchguard.com](http://www.watchguard.com).

©2013 WatchGuard Technologies, Inc. All rights reserved. WatchGuard and the WatchGuard Logo are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part. No. WGCE66791_120913