WHITE PAPER

FireEye

GAZING INTO THE CYBER SECURITY FUTURE:

20 Predictions for 2015

SECURITY
REIMAGINED

CONTENTS

Like the technology they exploit, today's cyber attackers evolve and innovate at breakneck speed. Keeping up with the latest techniques and tools is difficult for even the most advanced security teams. Anticipating future trends can be even harder.

We have a unique vantage point at FireEye. Our auto-generated intel from millions of FireEye network and endpoint sensors, our real-world experience from Mandiant incident-response cases, and our dedicated research team have a front-row seat to how attackers are compromising organizations and how their tactics are evolving.

Based on this experience, we've taken a crack at looking into our cyber crystal ball to think about what we can expect to see in 2015. These forecasts are more than an academic exercise. Think of them as guideposts on what to watch for in coming months. By knowing what threats are coming—from both a technical and business perspective—security teams can assess and bolster their defenses now.

TECHNICAL PREDICTIONS

1. **Windows-based remote-access tools (RATs) and backdoors migrate to OSX.**

   Apple's growing enterprise footprint will force attackers to adjust their toolset to broaden attacks across the OSX platform. That means we are likely to see more malware targeting OSX systems, which have been considered relatively safe from cyber attacks.

   Recommendation: If you have OSX users, include them in your security planning—everything from configuration management and patching to monitoring and incident response. Invest in technology to monitor threats to your OSX devices. FireEye has solutions to detect advanced threats that target OSX, including network and email appliances that can find previously unknown OSX threats.

2. **Mobile ransomware that steals cloud accounts and encrypts the data.**

   Mobile attacks will follow the Cryptolocker model, locking victims' files until they pay a ransom. This model proved effective and easy for attacks on traditional PCs and servers. Why wouldn't attackers try it on mobile devices?

   Recommendation: Consider carefully the value you get from cloud-based data security services. Keep a copy of files you really don't want to lose offline (encrypted USB sticks can be very useful for this), but be careful to safeguard the backup and your passphrase.

3. **Phone-based two-factor authentication becomes inadequate.**

   We'll see attackers targeting both PCs and phones or just the phone itself. Expect more campaigns like 2012's Eurograbber campaign. The series of attacks used a modified version of the widely used ZeuS toolkit to compromise phones and defeat two-factor authentication systems used in many banking systems. In all, cyber criminals stole 36 million euros ($47 million) from customers of more than 30 banks.[1]

[1] Bruce Sterling (Wired). "Eurograbber botnet deftly steals 36 million euros from banks." December 2012.

If your mobile banking app enables you to log in and receive a security code via text message, you're not protected. Essentially, your phone acts like a PC, so you need something else as the "second" authentication factor.

Recommendation: Given the huge variety of security problems with mobile phones, assume that they are not suitable as a primary security device. Only a device that is not connected to networks or other devices (a "non-promiscuous" device) should be considered safe for the strongest authentication requirements.

Perhaps smart watches or smart "whatevers" can solve, or at least mitigate, the problem. For example, Google users can buy USB-based security keys to make two-factor authentication easier and more secure. Soon, they may be able to use a mini-USB version for their mobile devices.

4. **The rate of "cataclysmic events" such as Heartbleed and Shellshock increases.**

   It won't be just one thing, but a combination of unrelated events that have the capability to destabilize "the Internet of things." Organizations need to get better at dealing with these storms.

   Recommendation: Have processes in place to audit your environment for vulnerable systems—and to get them patched quickly. Consider investing in packet-capture and network-forensics capabilities to enable you to look for attacks against newly announced vulnerabilities that have appeared before you could patch. FireEye technology lets you record all your network traffic and search for indicators of compromise (IOCs) in current and past network activity.

5. **Linux point-of-sale malware increases.**

   There is not a great deal of awareness or research around Linux-based point-of-sale (PoS) systems. Linux-based PoS systems are used all over the world; some are even free, open source, or far less expensive than Windows-based PoS offerings. These systems are appealing, but many operators lack the in-house expertise to address threats that target them and maintain proper configurations, updates, and so on.

   To date, most of the PoS malware we have seen is Windows-based and detected by the majority of big-name anti-virus software makers. As awareness of potential threats grow, organizations will become better at detecting them. But Linux-based PoS systems present a whole new playground for attackers—and could potentially be even more dangerous for victims.

   Recommendation: If you are running Linux-based systems for your operations, expect that they will become a target of opportunity for criminals. Major security bugs like Heartbleed and Shellshock are common on Linux systems. Understand the attack surface of your Linux hosts and the attack vectors they are exposed to. And have in place robust operational processes to manage, monitor, and maintain their security.

6. **PoS attacks will increase in frequency and hit a broader group of victims.**

   Speaking of PoS attacks, we will see new families of malware that will be available to a growing number of cyber-criminals and target a wider range of retailers.

   Criminals will always go where the money is, and nowhere in the realm of cybercrime is the risk-to-reward ratio greater than credit card information stolen from PoS systems. Expect to see more creative targeting as large retailers harden their defenses and more criminals get into the game looking for untapped potential victims.

This trend should cause attacks to spread to middle-layer targets such as payment processors and companies that manage and maintain PoS devices for large and mid-sized businesses. In these cases—as we've already seen with at least one customer—a single successful intrusion could provide access to pools of credit card data from many sources, rivaling the numbers stolen from any single retailer to date.

Worst of all, expect to eventually see increasing attacks at both mid-sized and smaller local businesses that have neither the resources to defend against this threat, nor the knowledge to detect and mitigate them once they occur.

Recommendation: If you are in retail or hospitality—or simply processing payment cards in any significant volume—you are likely to face attacks on your PoS systems.

Don't wait for it to happen. Make sure you've assessed all the attack vectors, have monitoring in place to detect attacks, and respond immediately when you find malware in your network. Don't assume that low- level malware means the attackers were too stupid to go after your PoS. They may intend to pivot from the initial attack to your PoS system after they breached your network.

7. Linux malware triggers an "Internet of Things" security problem.

The Shellshock-exploiting attack last fall on network-attached storage devices sold by QNAP is a perfect example of attackers targeting specific devices with Linux malware. We will likely see other popular platforms attacked, exposing a large pool of users and devices. As more vulnerable platforms are discovered, we can expect to see more specialized Linux malware that targets consumer and small-office/home-office devices.

Recommendation: Use basic hygiene with consumer electronic appliances—regularly upgrade the firmware when security patches are released, set strong passwords for administrative access, and block access from remote networks. Virtual currency mining has made consumer devices such as network-attached storage, Internet-connected TVs, and gaming consoles valuable to criminals who can turn your home device into a money-making machine.

8. New security threats for Internet-connected devices.

Hackers and researchers will spend more time evaluating the security threats from embedded devices by reviewing the firmware using tools such as Binwalk. That will create new potential attacks to consumer gadgets—and more awareness of the threat.

These days, most home users know that they should patch their computers. Soon, they will need to learn when their devices are vulnerable, how to download firmware from a vendor, how to log into their devices, and how to upgrade their firmware.

But until they do, malicious actors have a window of opportunity to exploit vulnerable devices to their advantage.

Recommendation: See our advice for Prediction No. 7.

9. **Use-after-free exploits decline.**

   Exploiting use-after-free (UAF) vulnerabilities will become more and more difficult, thanks to efforts by Microsoft to mitigate the threat. These efforts include techniques dubbed “delayed free” and “isolated heap.” Bypassing these software changes to exploiting the UAF vulnerability will require more skills and techniques that are more sophisticated.

   Recommendation: Keep your operating system and other software up to date.

10. **’Nix-side vulnerabilities (Unix and Linux) will increase.**

    In the wake of OpenSSL (Heartbleed) and BASH (Shellshock) vulnerabilities, expect a surge of “fuzzing”—throwing random data at applications to see what breaks. That means new Unix and Linux vulnerabilities to fix (or exploit).

BUSINESS PREDICTIONS

1. **Businesses stop paying for anti-virus software.**

   IT security organizations will stop paying the "big guys" for anti-virus (AV) software outright. Instead, they will deem Microsoft-provided AV as "good enough," especially since it's usually paid for already. This spending will shift to other endpoint solutions that address advanced detection, response, and forensics.

   Recommendation: If you haven't recently re-evaluated your security investments, do it now. We recommend that companies annually review the value they get from their security portfolio, taking into account both their organization's changes and the evolving threat landscape.

   If you have a Microsoft environment, consider using Microsoft Security Essentials. Also consider Microsoft's Enhanced Mitigation Experience Toolkit (EMET) 5.1 for even greater protection from known threats. Use the money you save to invest in technologies that help you prevent, detect, analyze, and respond to new and emerging threats.

2. **SIEM spending plummets.**

   After years of disillusionment with the low returns from their high investments in security information and event management (SIEM) tools, companies will begin to reduce their spending in this arena to the bare minimum for compliance purposes. They'll shift this spending to threat intelligence, data analytics, and emerging "SIEM next" solutions that aim for actual "security" in event management.

   Recommendation: After years of investing in more computing and storage, SIEM vendors are all jumping on the mantra of Big Data, as if this will magically fix all the problems with legacy SIEMs. Aside from compliance reporting, most of the money chasing SIEM is wasted, since SIEMs are not the sources of security problems.

   Organizations should look at how they detect new malware, how they can apply security intelligence to their environment in real time, and how they can speed security analysts to respond to security threats effectively and efficiently.

3. **Threat intelligence continues to be frothy.**

   Customer needs (and vendor capabilities) are not yet well defined. It's a new concept, still evolving. Expect to see more experimentation from established (but forward-leaning) players as well as new start-ups. You won't be able to turn around at RSA this year without seeing a "threat intelligence" vendor.

   The market for threat intelligence could splinter into three areas:

   - Tactical intelligence—the IOCs for minute-by-minute response
   - Operational intelligence: what you need to know to understand the latest threat (think daily threat briefings)
   - Strategic Intelligence—understanding the broader implications of threat actor changes, which guides where you spend your defense dollars

CISOs will seek out strategic intelligence, whereas tactical and operational intelligence will become staples of security operations centers (SOCs) and computer incident-response teams (CIRTs), respectively.

Recommendation: You need threat intelligence. But you need different types of intel for different use cases.

Tactical threat intelligence helps you to monitor, alert, and block known malicious behavior, content, users, and network connections. This needs to be automated, as this tactical information is constantly changing.

You need operational threat intelligence to help your security analysts better understand the context of an attack, what the attacker is likely to do next, and how you can best reduce the business impact of the attack.

And you need strategic threat intelligence to better understand the evolving threat landscape and guide your investment in security controls where it will give you the best return.

The key to all this is that the intelligence itself must be actionable. Look for vendors that provide not just the intelligence itself, but the ability to use it. If you can't make a decision based on the intel you received, it's no better than noise. Threat intelligence on its own is largely wasted. You need it to be connected with your automated controls (tactical), security analyst's processes (operational) and security leadership decision-making (strategic).

4. **Fraud goes mobile.**

   With Apple Pay joining Android and others in the mobile payment space, near-field communications (NFC) technology is becoming mainstream. We will see a renewed vigor and focus on cybercrime in the mobile market as criminals prepare to follow the move to mobile payments.

5. **Supply-chain attacks increase.**

   As large organizations continue to adapt their cyber security, the gap between their best practices and mainstream practices will grow. That disparity will drive attackers to compromise less mature companies and use them as the entry points into more mature enterprises they're connected to. Consequently, understanding the supplier ecosystem will become an increasingly key part of cyber strategies.

   Recommendation: Your business can require suppliers to show evidence of good security controls. Building security requirements into your master service agreements can push your suppliers to improve their security. And requiring them to demonstrate the effectiveness of their controls is a good way to make sure that your supply chain is following through on their security promises.

   Ask for metrics of security effectiveness such as mean time to detecting new threats, and mean time to resolving them. Most companies can't do this today, so start with requirements, then build reporting requirements into your contracts over time.

6. Cyber insurance becomes a key part of cyber security plans.

Amid a growing volume of high-level breaches, businesses will look for new ways to minimize the business impact. Cyber insurance will become an increasingly popular option.

This trend will drive insurers to ensure that policy holders are taking reasonable steps to avoid major claims. As insurers take a closer look, we should start to get a clearer idea of real-world cyber hygiene standards and the actual impact of cyber threats by industry and geography.

Recommendation: You can only really insure the gap between what your security controls can and cannot protect. Insurance companies are going to make sure that they only pay out on attacks and damages you could not reasonably have prevented. So the most important things you can do are to understand the size of your "attack surface" and deploy effective controls to monitor, manage, and protect it.

Insurers may pay out large claims in the event of a cyber security failure only after policy holders demonstrate they had taken all reasonable precautions to prevent it. Insurance, therefore, becomes the bridge across the security gap—it's still up to you to ensure the gap is as small as possible.

So if you don't already have a demonstrably effective security program in place, cyber insurance may be wasted money. Security consulting firms can expect to profit from this—from both the companies looking to show that they are insurable and insurers seeking evidence that claims should not be paid.

7. More incident response plans fail, with greater impact.

Many companies fail to regularly test their cyber incident response plans. Amid increasingly high-impact breaches from targeted attacks, response teams with inadequately tested and rehearsed response processes will buckle. This could result in a major brand going out of business in 2015—not because the attack is technically exceptional, but because of the victim could not respond effectively.

Recommendation: FireEye has redefined what "winning" means in cyber security. An attacker can succeed very easily against most companies today. Even the best-prepared organizations continue to suffer security breaches.

Breaches are inevitable if you are sufficiently large and valuable as a target. But the impact of a breach is not.

Winning against an attacker means identifying attacks before they succeed, detecting when they do breach your defenses, and eliminating them from your systems before they can cause lasting harm. While you can't prevent every breach, you can avert the worst consequences.

8. Fewer organizations run their own security operation centers.

As the sophistication and impact of cyber threats continues to increase, only the best-funded and efficient organizations can build and operate a security operations center (SOC) with the scale and skills needed. More organizations will recognize the necessity. But lacking the ability to build their own SOC, many will seek out managed services.

Recommendation: Are you prepared to spend tens of millions of dollars every year on building, maintaining, and operating your own SOC? If not, you can't expect to maintain the capacity and capability you need to effectively protect your business. Consider looking at ways to get your SOC capability as a service by partnering with organizations that have the scale, expertise, and resources to operate a SOC on your behalf. Operating a sub-scale SOC yourself will likely cost you more and give you less return for your investment.

9. Mindsets change from a peacetime to wartime footing.

The public is now acutely aware of the impact of attacks, thanks to the near-constant news headlines of the last year (Target, Home Depot, JPMorgan, Japan Airlines, and so on). This knowledge, coupled with business owners recognizing that security breaches are much more than a nuisance, will lead organizations to fundamentally change how they think about cyber defense.

They will shift away from compliance (where you spend money on audits and still lose your shirt) towards security that focuses on actual threats (because the UN, Interpol, the World Trade Organization, and Father Christmas aren't going to save you from attacks).

Fortunately, we expect compliance standards (PCI, HIPAA, FISMA, etc.) to get revamped as the world realizes that being compliant doesn't mean you are secure.

Recommendation: Adopt a mindset that focuses on threats rather than compliance, and consider what your security organization needs to change to prevent, detect, analyze, and respond to real threats.

Change your goal from demonstrating compliance to identifying IOCs. Collect intelligence from security attacks to better understand the attacker, detect attack campaigns, and identify the motives of attackers targeting your organization. Use this information to improve your defensive posture, target your security investments, and ultimately improve the protection you provide to your business.

10. Security spending continues its shift from prevention alone to a mix of prevention, detection, analysis, and response.

Historically, most security spending has been dedicated to the people, processes, and technology to prevent attacks. A growing number of security leaders have become aware that prevention is necessary—but not sufficient—to fully protect the organization.

As more and more organizations become aware of the need to detect, analyze, and respond to intrusions, security spending will follow suit. This trend acknowledges that breaches happen, but that detecting and responding to them before they cause lasting harm is what really counts.

Recommendation: If your organization doesn't know how it is going to detect and respond to security incidents, that's where you need to increase your investments. Redefine security from preventing threats to preventing the worst impacts of those threats. You reduce or avoid the worst consequences only by detecting security incidents that have bypassed your perimeter controls—because they will—and responding quickly thoroughly.

Have a security program that can detect threats, including those that get through your perimeter defenses. Then look to strengthen your response capabilities with the right technology, intelligence, and expertise.

Find ways to collect information to speed your incident response, such as endpoint threat detection and response tools (for example, the FireEye Endpoint Threat Prevention Platform). And make sure your analysts have the right intelligence and education to understand how to stop an attack that has penetrated your perimeter defenses.

CONCLUSION

As the technology landscape evolves and attackers continue to adapt, we're going to see new vulnerabilities to mobile, new operating systems and the cloud—and new ways for attackers to exploit these weaknesses. Preventing every breach is impossible. So acting now to assess your vulnerabilities and weak spots is critical.

The best way to mitigate damage from a breach is to develop and implement detailed mitigation plans ahead of the intrusion—and to invest in solutions that alert at the first sign of a breach.

About FireEye

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. The FireEye Global Defense Community includes more than 2,700 customers across 67 countries, including over 157 of the Fortune 500.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**

FireEye