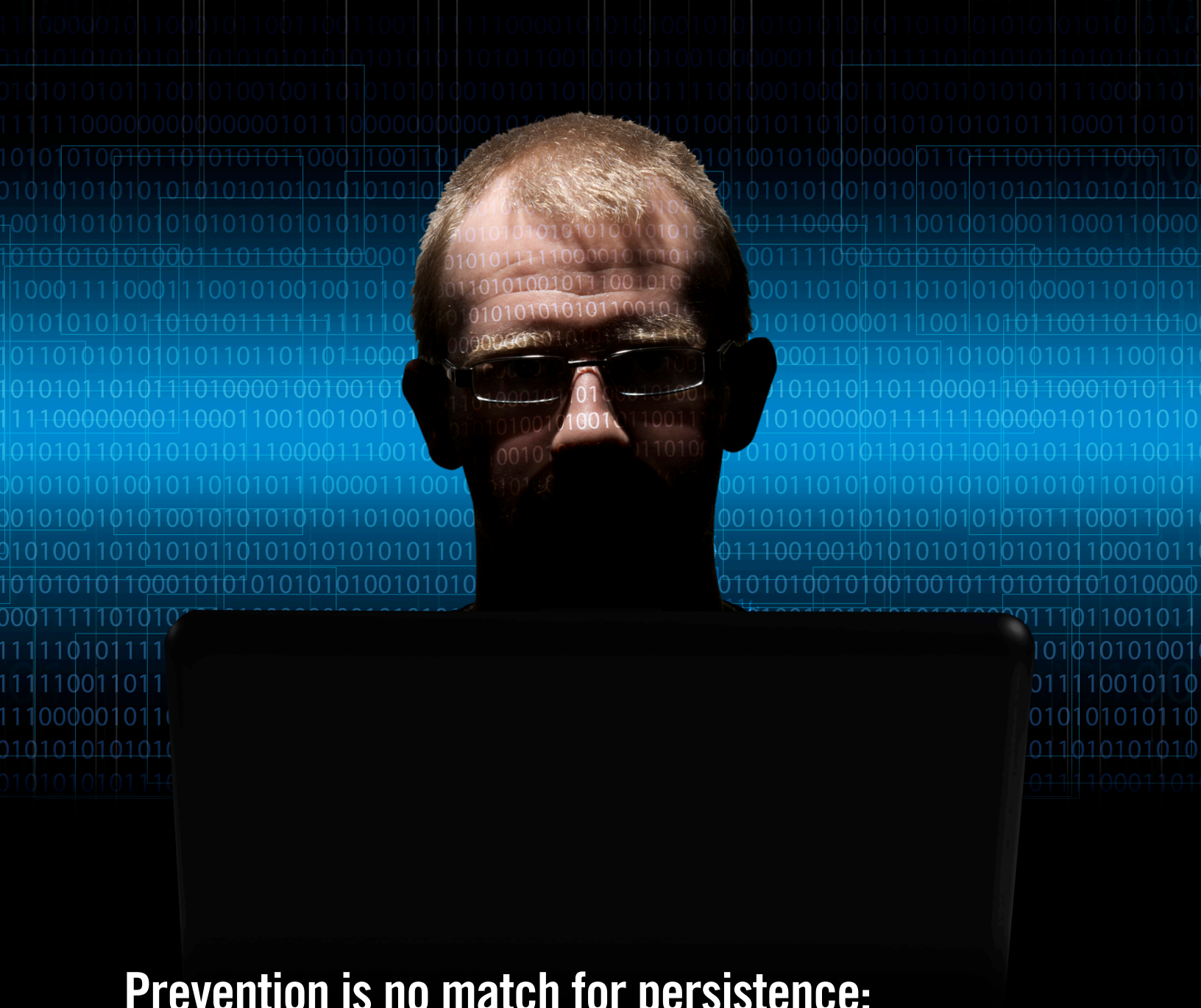


Prevention is no match for persistence:

Rethinking Cyber-Security in the Age of Relentless Attacks

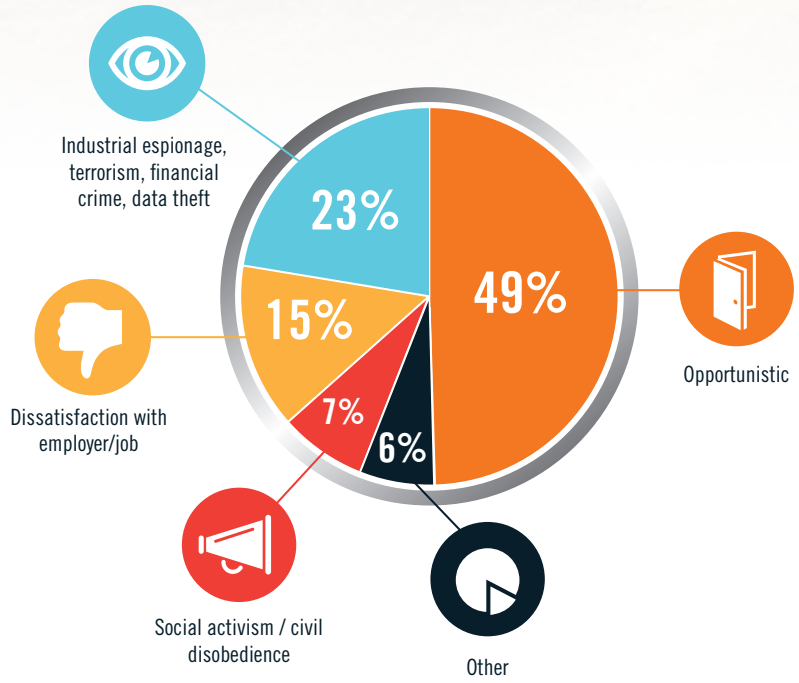
OpenDNS

CYBER-INSECURITY:
ARE WE DRAWING LINES IN SHIFTING SANDS?

Today, most IT security is based on prevention – an attempt to create counter measures against previously identified tactics and threats. In theory, understanding how hackers attack us helps us prepare our best defenses against them.

But in practice, we can never build our virtual walls high or strong enough to serve as sufficient barricades. For starters, old tactics evolve and new tactics emerge at a rate impossible for security professionals to match. Spear phishing targets our most vulnerable employees and watering holes attract the unwary. Our best "sandbox" malware analyses can miss some of the latest suspect behaviors. It's impossible to predict when and where the technologies we rely upon, such as Flash or Java, will suffer the exploitation of a previously undetected (a.k.a. zero-day) vulnerability.

Worse, practice makes perfect. The key part of any advanced persistent threat (APT) is the persistence; even relatively basic, "off the shelf" malware can become powerful when it is applied repeatedly across a wide attack surface. As our digital borders, via private and public cloud services and mobile users and devices, expand they become more porous and our digital line in the sand becomes too big to defend.



Relatively unsophisticated opportunistic attacks serve as reconnaissance for stronger, more targeted assaults.

SOURCE: IBM Security Services Cyber Security Intelligence Index

For enterprises or organizations at any scale, prevention alone can never be a sufficient defense: our security professionals must be right and fast all the time, but cyber-attackers just need to be effective once, over any time period.

Our new cyber-security environment demands a new way to think about our cyber-security strategy, one that aligns our security investments with our business risks, and is less centered on ideal prevention and more focused on reality: hackers represent an ever-present threat who cannot be intercepted by preventive techniques alone.

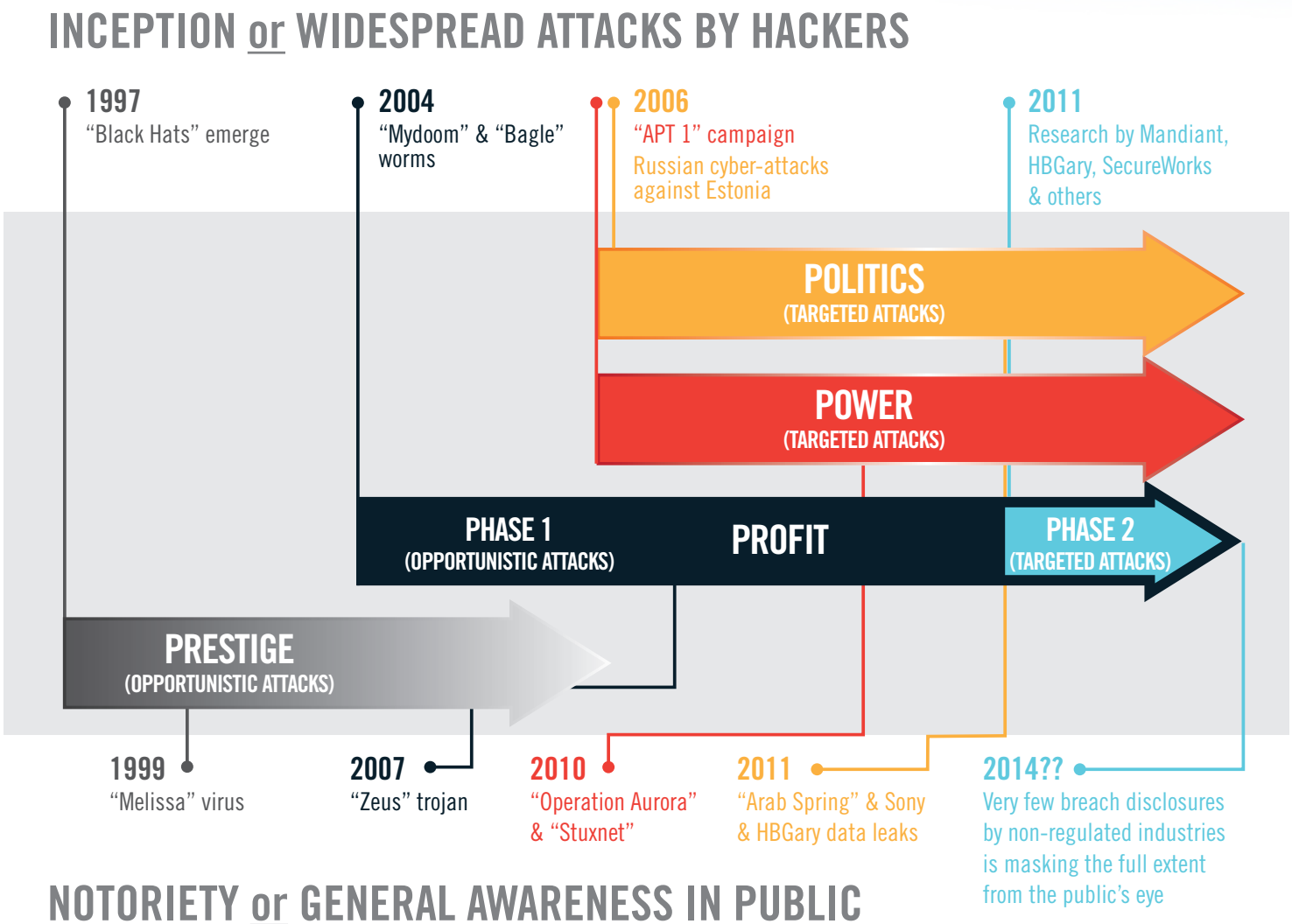
In the following pages, we will investigate the changing motivations of cyber-attackers – who they are and what they want – and explore the most promising strategies for combating them by complementing prevention with methods that reduce the impact of security breaches and increase the effort required to make them.

> *"There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again. Maintaining a code of silence will not serve us in the long run."*
>
> Robert Mueller
> *FBI Director*

DIFFERENT MOTIVES, BUT CONVERGING METHODS

About whom should we worry? For most small businesses to large enterprises, the answer seems simple: the cyber-criminal seeking profit. Motivated by money, these criminals or criminal organizations want to break in and steal monetizable data, such as personal identity information or intellectual property, that they can use to extract cash or sell.

An often ignored category is the nation state motivated by power and the "hacktivist" motivated by politics. Since the nation state seeks long-term strategic goals, and the hacktivist wants to score ideological points, they have been seen as largely inconsequential by businesses who do not believe they would be likely targets for either group. But techniques developed by one category can be, and are, adapted by the other two. The attacks launched by the nation state and/or the hacktivist today are being applied by the cyber-criminal as well. In fact, the discrete categories of attacker and motivation are beginning to merge, evolving into a new breed of cyber-mercenaries capable of applying multiple attack methods on behalf of any party motivated to hire them.



Today's cyber-mercenary learns from every kind of attacker, and is prepared to apply any kind of attack.

Evolving motives have led to the convergence of attacker techniques.

The Expanding Tactical Toolbox

As criminals, nation states and hacktivists learn from each other, they share many techniques in common:

Malware: weak or strong, it's dangerous

We may feel most threatened by the complex, custom-built malware developed by organized cyber-criminals. But the off-the-shelf black-market malware favored by many nation states, and the "script kiddie" tools used by hacktivists, can be equally effective – and dangerous. Persistent application of even weak malware can get attackers in the door.

Exploited Openings

Social engineering – the exploitation of human nature and behaviors – can create breaches even the most advanced technical engineering cannot make. Techniques such as spear phishing (pushing malware to employees or other associates through email) or watering holes (poisoning attractive Websites with malware) enables bad actors to get a foothold and create "backdoor" entrances to otherwise well-protected systems. Once inside, attackers can make lateral moves within the system through command-line tools, passing of credentials, compromises to the authentication system and other techniques to gain even greater access to more sensitive data.

Vulnerable endpoints

In the Second World War, the Germans discovered an excellent way to "break" France's Maginot Line: they simply went around it. Likewise, attackers find it easier to approach heavily defended corporate networks by forgoing direct attacks for assaults on the periphery, the less secure employee endpoints of laptops and mobile devices connected to insecure public Wi-Fi networks, less secure remote branch offices, or internationalized versions of enterprise Websites. When security policy fails to look beyond core systems, the resulting lack of coverage leaves related endpoints exposed to attack.

Prevention Alone Cannot Solve the Problem

Unfortunately, cyber-defense has been largely reactive in nature, a preventive effort based on counter defenses to previously experienced attacks: antivirus signatures for malicious executables, email filters for unwanted messages, Web filters for compromised sites, reputation systems for suspicious files or IPs, sandboxes for malicious behaviors, and so on.

But these preventive measures are undermined by hard realities:

Time is not on our side

With a median detection time (from system intrusion and network breach to awareness of it) estimated at anywhere from 300 to 400+ days, much of the damage has been done before we can do execute a counter-measure against the attack.

Our silence increases their invisibility

Private businesses, adverse to bad publicity and sensitive to brand reputation, are reluctant to admit damage. According to many studies, as few as 2% - 30% of businesses disclose their breaches. Many that do are selective about what they disclose; others reveal only what they are legally obliged to. This lack of disclosure provides a cloak of invisibility that helps conceal the nature and volume of cyber-attack activity. Conversely, the attacks that are disclosed may be disproportionately scandalized by the media, misleading us as to their actual scale.

The perimeter is too porous

The line between private and public has virtually dissolved; today, corporate data may be stored in cloud applications and may roam with employees' "bring-your-own" laptops and mobile devices, expanding the attack surface. Other boundaries are porous as well: your network might be a stepping-stone to a more desirable target; conversely, other partner environments, such as those of your supply chain vendors, may be gateways into yours.

Who do you loathe?

Today's corporate networks are up against a world of potential attackers with various interests, yet increasingly common methods of attack.

East European Hackers:

- Well-educated, well-organized and well-equipped to launch sophisticated attacks
- Lacking access to high-paying jobs commensurate with their skills, they are attracted to criminal organizations that pay well and, in practice, are indistinguishable from legitimate businesses
- Have a clear understanding of the digital trails they leave behind – and of an enterprise's ability to detect them
- Brazil is following this model and is emerging as a player in this cyber-criminal landscape

---

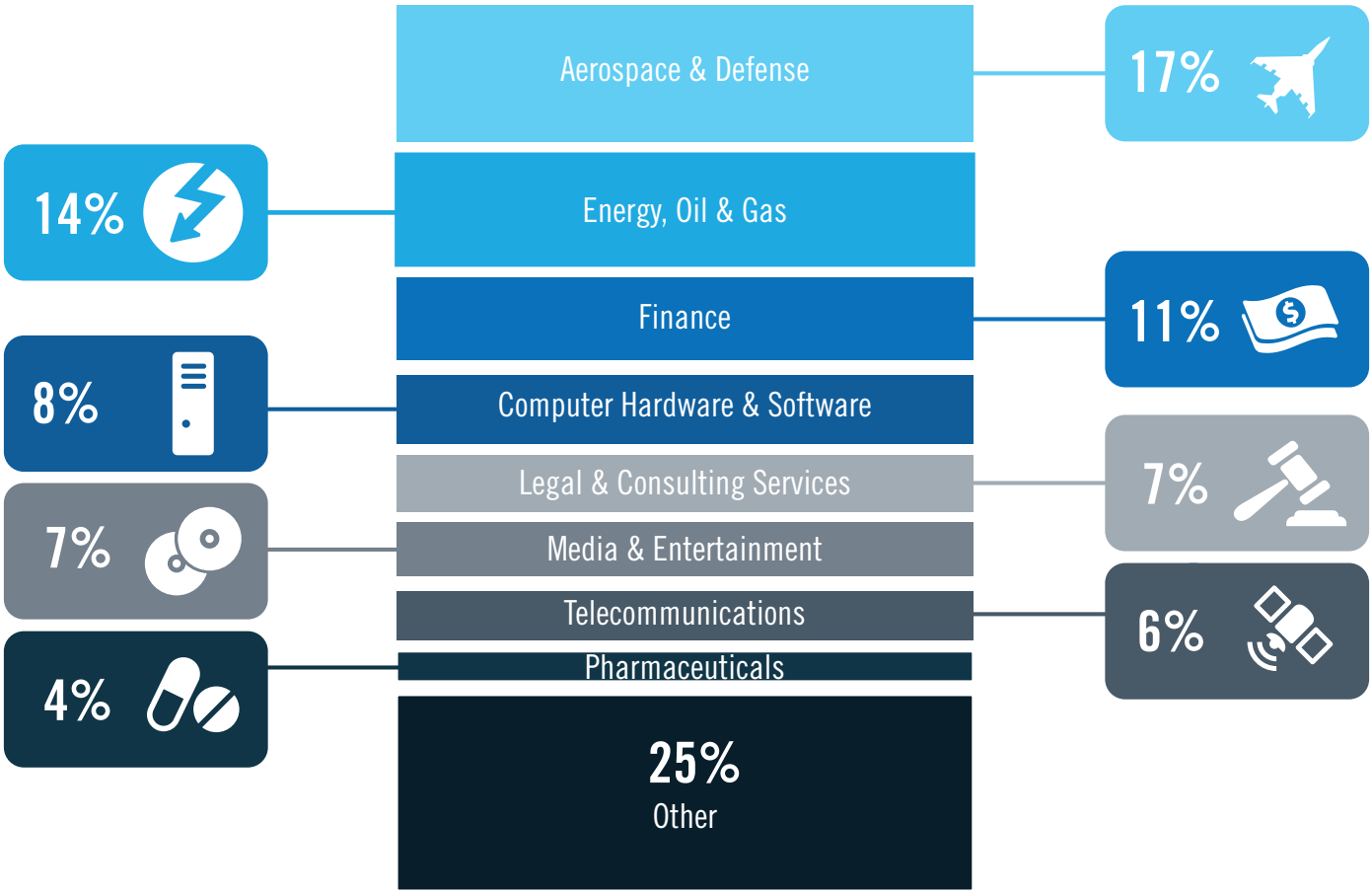
East Asian Hackers:

- Patriotic and professional, they work in collusion with nation states who see cyber-activity as a low-cost means of achieving military/economic/political ends
- Leverage reconnaissance and planning to work their way up from vulnerable targets to higher value assets
- Many Middle Eastern nations are now following this model

North American & Western European Hackers

- Individualistic and often idealistic, these hackers operate within loose meritocracies without centralized controls
- Varying levels of technical expertise, matched to limited financial resources
- Generally fights decreasing privacy and increasing corporate and/or government control

Industries Being Targeted by Advanced Attackers



SOURCE: Mandiant M-Trends Report 2013

Today, no enterprise is immune from the advanced attacks that may have been initially designed to penetrate nation states and sensitive industries, but can be applied to any network, anywhere.

> *"Small attorney firms or professional services firms are getting compromised because they have sensitive data on clients. So rather than try to breach a large, well-defended network, it's easier just to compromise the outside counsel or auditing firm, and get financial statements or plans for MAs [mergers and acquisitions] or other trade secrets from those firms."*
>
> Kyle Maxwell
> *Senior Analyst with Verizon*

RETHINKING CYBER-SECURITY TO INCLUDE DETECTION AND EDUCATION

Prevention will always play an important role in cyber-security. But given both the scale of our network perimeters and the persistence of attacks, prevention alone is an unrealistic intervention. Instead of pursuing the impossible – perfect prevention – we must reinforce the practical: a strategic approach to cyber-security that complements preventive efforts with quick detection and containment of breaches, and proactive education and "complication" that makes breaches more difficult to exploit.

As cyber-attacker motives and means converge, business networks should embrace a more comprehensive security model that pursues three objectives:

1. Reduce the **risk** of security breaches through predictive defense and prevention.

2. Reduce the **impact** of security breaches through quick detection and containment of assaults.

3. Increase the **effort** required to breach security through proactive education among network users, and by employing technologies that make it more difficult and expensive for attackers to work in your environment.

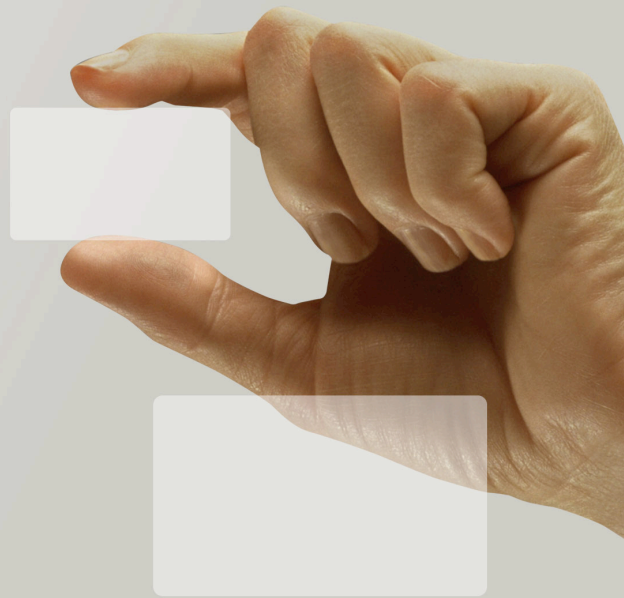
I. Predictive defense and prevention

The most familiar of the three elements to cyber-security strategy, predictive defense and prevention applies lessons learned from previous attacks to deploy techniques that reduce the likelihood of successful assault. The crucial components of this strategy are:

Reduce the attack surface

Given that many cyber-attacks do not involve advanced malware, but look for easy opportunities to exploit weak spots, it makes sense to reduce the overall "surface" exposed to attack. Hackers look for unpatched vulnerabilities, easily guessed or popular passwords, and low-level users who have access to high-value assets and/or servers. To fight back, security professionals should consider:

- Enforcing strong passwords
- Implementing the "least privilege" principle: access to particular information, processes and programs should be restricted to those with legitimate needs
- Performing regular vulnerability scanning and patch management
- Using VLANs (virtual local area networks) to segregate traffic types, isolate services, and apply hardened network configurations



Layer threat protection

Once inside your system, hackers often make lateral moves from the easy entry-points to more valuable assets. By layering threat protection, you can erect more barricades, making your systems more difficult to infect and networks more difficult to breach. Techniques include:

- Uniform implementation of security solutions across all network access points, including remote offices, roaming IT- and user-owned devices
- Matching your security technologies to your threats: meet known commodity threats with signature-based solutions; address known advanced threats with signature-less solutions; and face unknown advanced threats with predictive solutions.

II. Quick detection and containment

Despite our best efforts, persistent attacks will penetrate our preventive defenses. But we can minimize the impact of these invasions by taking measures to rapidly identify and contain breaches when they occur. Quick interception requires you to:

Obtain coverage and visibility

When our network perimeter is greater than the network itself, by virtue of data stored in the cloud and devices used off the network, then security becomes less a matter of control and more a matter of visibility – seeing what the breaches are and where they are coming from. As a matter of habit, we should:

- Implement security enforcement everywhere we can, not just in our network, but within our cloud-based services and on employee-owned or used mobile devices
- Aggregate logs and security events from multiple solutions into one point of visibility through a security information and event management (SIEM) system

Monitor network activity

The “phonebook” of the Internet, the domain name system (DNS) is not only the standard by which names and addresses are linked, it is a potential point of manipulation that can be exploited by hackers. But DNS cannot be simply locked down – the Internet cannot function without a fast, broadly available domain name system. We can contain threats by:

- Leveraging cloud DNS monitoring tools to watch externally-facing DNS infrastructure and detect changes to DNS records
- Enabling extra security features offered by DNS registrars, such as locking domain name registration information
- Running a performance monitor on internal DNS servers to count the number of recursive queries per second servers are forwarding
- Logging and analyzing recursive DNS queries to detect anomalous activity patterns from infected devices

III. Proactive education and complication

The third strategic element helps fill in the security gaps that cannot be sufficiently addressed by the other two. Reactive defenses may be undermined by the sheer volume of cyber-attacks; quick detection and containment can be compromised the difficulty of collecting, analyzing and acting upon security event logs in a timely way. By taking pains to educate network users (usually the weakest link in any system) and to inhibit the spread of damage once a breach has occurred, you can frustrate hacker attempts to reach your most valuable assets. Components include:

Raise security awareness

Human behavior represents a double-pronged security threat: it resists our best efforts at control, and it opens up avenues of attack – from data scored on social media posts, friends' email accounts, and Website activity – that hackers can use to their advantage. Fighting ignorance with information is vital to minimizing human error. You can help change employee/associate behavior through:

- Attack simulation exercises that both teach awareness and test safe online behavior skills
- Internal IT security marketing campaigns
- Short IT security training sessions – not just one-offs to tackle the latest scams, but regular events that keep users alert

Employ mitigation methods

While opportunistic attacks are pervasive, they are, by definition, easily discouraged; when an attempt fails, hackers tend to move on. When hackers persist, each of their attempts increases the likelihood of discovery. Either way, imposing obstacles helps tilt the advantage in your favor. To make hacking more difficult, you can:

- Encrypt data at rest and in motion
- Use customized operating systems or virtualized web browsers
- Work with operating systems and software vendors that enable data execution prevention (DEP) and address space layout randomization (ASLR) to increase hacking costs and decrease hacking ROI

> *"Larger corporations have upped the ante against cybercrime recently, investing heavily in sophisticated security strategies. That's forced cybercriminals to look for other ways in."*
>
> CNN

REPLACE "SILVER BULLETS" WITH SOUND STRATEGY

It's natural to wish for a simple solution to our complex cyber-security challenges. But instead of putting false hope in one "silver bullet" defense tactic, it's much more productive to think deeply and act broadly – to analyze our risks, assess our investments, and craft a multi-tiered security strategy that will defend our networks effectively and efficiently.

While there may be no easy answers, asking the right questions can help us craft appropriate plans. Consider the following worksheet of security issues as a productive step toward identifying your best strategy for intercepting attacks and taking corrective action.

1. Given the nature of your organization, who are your most likely attackers?
2. Which of your assets align to attacker motives?
3. Where are the vulnerabilities among your assets, supply chain vendors, partners, services providers and customers?
4. How secure are your assets on the cloud – or on the devices your employees use?
5. How might these vulnerabilities be exploited?
6. What preventive tactics are currently in place and how effective are they?
7. Have you taken measures to reduce your overall attack surface?
8. Have you applied consistently high security standards throughout your organization?
9. Do you have visibility into cloud and DNS activity that could affect your network, your system, your data?
10. Have you made sufficient investments in education and training among your employees and partners?
11. Based on your assessments of the above, which tactics/techniques would be most likely to minimize and/or mitigate the impact of an attack?

Predict, Prevent, Contain and Obtain Visibility into Emerging Threats Before They Happen

Organization by organization, security tactics will vary by various needs, risks and requirements. But one thing remains constant: the need to take action before threats become breaches. Consider the power of an Internet-wide layer of threat protection that:

1. Enforces security on every device, everywhere, regardless of location, whether or not they are connected to your network, communicating over the Web, or over non-Web connections
2. Probes beyond hacker tactics and techniques with intelligence and enforcement that focuses on the Internet origins of malware distribution and botnet command and control infrastructures
3. Gathers global intelligence and situational awareness from a tremendous volume, velocity and variety of data – data that reflects live patterns of global Internet activity across a statistically significant number of Internet users and connections every day

Add Predictive Intelligence, Threat Protection, and Security Enforcement Everywhere

Today, over 50 million daily-active users across 160 countries point their DNS traffic to the OpenDNS Global Network – with 100% uptime since inception in 2006. And every second, the OpenDNS Security Graph acquires and learns from over 1 million malicious and non-malicious Internet events. This global intelligence and situational awareness – reflecting over 2% of the world's Internet connections – is used to predict, prevent, contain and obtain visibility into emerging threats before they happen.

Umbrella is a cloud-delivered, DNS-based security enforcement platform that protects every device, everywhere. Using OpenDNS's predictive intelligence, it blocks more than 80 million security events every day. It takes less than 30 minutes to deploy and less than 1 minute to view all the Internet activity occurring across your entire organization.

Visit OpenDNS.com to Instantly Start a Free 2-Week Trial

OpenDNS

OpenDNS, Inc. www.opendns.com
1.877.811.2367