FEATURE

Sometimes, Cyberattackers Are Going to Get In

The State of Cybersecurity 2018

The cybersecurity problem in a nutshell is that criminals are launching cyberattacks against the global attack surface comprised of the world's people, companies, governments, banks, power grids, utilities, hospitals, schools, data centers, servers, networks, personal computers (PCs), laptops, tablets and smartphones. Add Internet of Things (IoT) devices and the targets expand to cars, medical devices, kitchen appliances, thermostats, TVs, wristwatches, webcams and more.[1]

Cyberattacks on these devices and systems are the result of two distinct types of cybercrime that emerged in 2016. Traditional mass-market cybercrime groups carried out large-scale email campaigns to distribute commodity malware such as ransomware and online banking threats. Their distribution methods shifted away from web-based exploit kits to more traditional methods, in particular, the use of email attachments. The other side of cybercrime is made up of organized criminal groups responsible for a number of sophisticated financial heists.[2] It must also be acknowledged, with Edward Snowden and WikiLeaks files as examples, that nation-states do their share of hacking too.

The prevalence of low-hanging fruit for cyberattackers to exploit continues to grow. There are no trivial systems in the network. Across different applications, operating systems and insecure deployments, cyberattackers are looking for the easiest way to gain entry.

Figure 1 states some sobering cybersecurity facts.

Next, some of the basic principles behind cyberrisk are reviewed by first distinguishing between information, IT and cybersecurity.

Information Security Defined

Information is data that are:[3]

- Accurate and timely
- Specific and organized for a purpose
- Presented within a context that gives them meaning and relevance
- Able to lead to an increase in understanding and decrease in uncertainty

Figure 1—Cybersecurity Reality Check

Every company is under constant cyberattack, certainly by chance, other times as a direct target.
Enterprises are predictable because cyberattackers know human weaknesses and the technologies used.
Cyberattack offense is easier and less expensive than defense.
Cyberattack offense just has to get lucky once. Defense must be lucky always.
Senior management thinks cybersecurity is an IT problem. (It is not.)

The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standard ISO 27000:2016 defines information security as the preservation of confidentiality, integrity and availability of information.[4] In addition, other properties, such as authenticity, accountability and nonrepudiation, can be involved.

IT Security Defined

IT security can be defined as the technologies that protect information at rest and in transit from point of origin to point of destination in an IT environment. Firewalls provide the best example of IT security.

Keith Price, CISM, CGEIT, CISSP
Is director and principal consultant at Black Swan Group based in Sydney, Australia. He specializes in cybersecurity risk management, strategy and assurance. His approach to cybersecurity is based on a 30-year multidisciplinary IT career across information security, IT risk, enterprise architecture and security program management. Price is a former director of the ISACA Sydney (New South Wales, Australia) Chapter.

Cybersecurity Defined

"Cyber" is derived from cybernetics, the study of communication and control systems in living beings and machines. *Cybernetics* was the title of a book written by mathematician Norbert Wiener in 1948.

"Cyber" can be added to (almost) any word to create an Internet reference (e.g., cybersecurity, cyberspace, cybercrime, cyberwar).

ISO/IEC 27032:2012 defines cybersecurity as the "preservation of confidentiality, integrity and availability of information in the cyberspace."[5] Cyberspace is the interaction of people, software and services on the Internet. For this article, cybersecurity is a single catch-all term meaning the protection of the use of cyberspace from cyberattacks.

Threat-Vulnerability-Consequences Defined

A cyberattack is where a threat agent exploits a vulnerability resulting in a negative impact. It is difficult to point to a recent example where a cyberattack resulted in a positive outcome for the target organization.

In cyberspace, threat agents are criminals using manual attack methods or automated malware to take control of the target IT systems. The common term for this type of threat agent is "cyberattacker."

A vulnerability is a weakness in a control. A control is any policy, process, practice, device or other action that modifies risk. The primary cybersecurity vulnerabilities are people and technology.

There must be a vulnerability for a cyberattacker to exploit, or a cyberattack will not be successful. No one can control somebody on the other side of the world cyberattacking the organization's online presence. The vulnerability footprint must be reduced through controls.

> "VULNERABILITY REMEDIATION SHOULD BE BASED ON A PRIORITIZED APPROACH—A TRIAGE WHERE THE MOST CRITICAL VULNERABILITIES ARE ACTIONED FIRST."

The US National Institute of Standards and Technology (NIST) defines the control families shown in **figure 2**. Many of these control families include varying combinations of prevention, deterrence, avoidance, detection, correction and recovery controls.

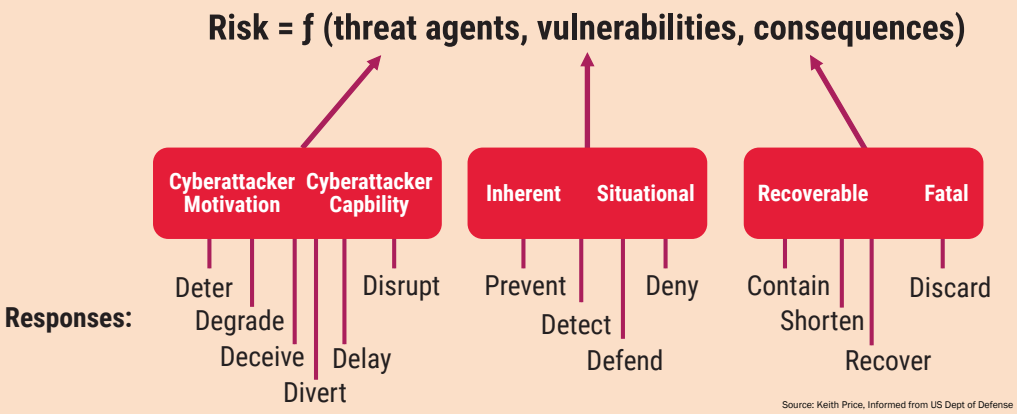
It is not possible to eliminate all cyberrelated vulnerabilities in people, processes, technologies or enterprise governance. The goal then should be to remove as many vulnerabilities as is practical. It makes business investment sense to reduce the cyberattack surface and the risk of a successful cyberattack. Vulnerability remediation should be

Figure 2—NIST Control Families

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Source: National Institute of Standards and Technology, Special Publication SP800-53 Rev. 4, USA, 2013. Reprinted with permission.

Figure 3—Risk Response to Three Cyberrisk Components



based on a prioritized approach—a triage where the most critical vulnerabilities are actioned first. The Commedon Vulnerability Scoring System (CVSS) provides an open and standardized method for rating IT vulnerabilities and determining the urgency of response.[6]

Cyberrisk Defined

Risk is simply the effect of uncertainty on objectives. An effect is a deviation from the expected and can be positive or negative. With cyberattacks, the effect is almost always negative.

A cyberrisk is a function of cyberattackers, vulnerabilities and negative consequences. **Figure 3** highlights various risk responses to these three components of cyberrisk threat agents, vulnerabilities and consequences.

An organization's cyberrisk appetite is a critical component of the enterprise risk management framework. As with market, credit and other operational risk, the board of directors is responsible for establishing the cyberrisk appetite for the organization.

How Big Is the Cyberrisk Problem?

It is a huge problem that is not getting any better any time soon. Security practitioners with long tenures have been watching attacks on computer systems grow exponentially since the late 1990s (though there were computer attacks long before then).

It has been said that, "Cybercrime is the greatest threat to every company in the world."[7] Cyberbreaches made public can expose an organization to recriminations of failed IT, information, cyber or governance controls. Damage to brand and reputation emerged as the top-ranked risk in Aon's recent Global Risk Management Survey.[8] Cyberattacks and related incidents have been entering the global risk landscape as among the most likely and potentially most impactful risk scenarios for the past two to three years. In North America, cyberattacks rank as the most probable risk. The failure to understand and address risk related to technology, primarily the systemic cascading effects of cyberrisk or the breakdown of critical information infrastructure, could have far-reaching consequences for global enterprises, economic sectors and national economies.[9] **Figure 4** lists some questions organization directors should be asking to start learning about their current cybersecurity state.

Figure 4—Questions Directors Need to Ask

Have we been the recent victim of a cyberattack?
Which of our digital assets are most at risk?
What is our worst-case scenario of a data breach?
How do we know our cyberdefenses are effective?
What is the extent of cyberattacks in our industry?

The Identity Theft Resource Center reported that there were 1,093 data breaches in the United States alone in 2016.[10] In the biggest data breach in history,

Yahoo reported in 2016 that more than 1 billion user accounts were exposed (through breaches that occurred in 2013 and 2014).[11] In October 2017, Yahoo gave an update that all 3 billion of its user accounts at the time of the breaches were exposed.[12] And for the most recent large-scale cyberattack, and one of the most damaging in the long term, the credit reporting agency Equifax announced in September 2017 that the personal data of 143 million US consumers had been compromised.[13]

While the occasional particular cyberattacker is arrested, in reality, there is no effective law enforcement in the world today for controlling cybercrime.

> "WHILE THE OCCASIONAL PARTICULAR CYBERATTACKER IS ARRESTED, IN REALITY, THERE IS NO EFFECTIVE LAW ENFORCEMENT IN THE WORLD TODAY IN CONTROLLING CYBERCRIME."

The sobering reality is that cyberattackers are one step ahead of defenders. The development and optimization of malware toward profit will remain the main parameter for attack methods, tools and tactics. Efficiently managed flexible tools continue to be widely available on the criminal underground.[14] The numbers that are available on breaches and records stolen in 2016 are eye-opening and, once again, show that cybersecurity efforts are not preventing these attacks from being successful.[15] While there has been a marked acceleration of both the aggressiveness and sophistication of cyberattacks, defensive capabilities have been slow to evolve and respond. A majority of victim organizations and those working diligently on defensive improvements are still lacking fundamental security controls and capabilities to either prevent breaches or minimize the damages and consequences of an inevitable compromise.[16]

Who Are These Cyberattackers?

There are several different types of cyberattackers. These include:

- Organized cybercriminals
- Hacker entrepreneurs
- Malicious employees
- Hacktivists (radical activists such as Anonymous)
- Nation-states
- Employees (unintentional)
- Third-party service providers (unintentional)

While not cyberattackers in a criminal sense, unintentional actions by employees, contractors and third parties can and do result in significant data breaches. Research in 2016 found that 68 percent of insider security incidents were the result of employee or contractor negligence.[17]

Cybercriminals are the most active threat agent group in cyberspace, responsible for at least two-thirds of the registered incidents.[18] In 2016, financial gain and espionage were still the top two motives, combining to account for 93 percent of breaches.[19]

Hacktivist protests have been on typical activist themes such as environmental policy, discrimination, corruption, pacifism, public health issues, support of minorities and media. Hacktivists activities may be considered stable over the past few years, causing low to medium impact damage through denial-of-service (DoS) attacks, data leaks and defacement campaigns.[20]

Figure 5 lists the factors that should be considered to determine the risk from each type of cyberattacker.

Figure 5—Cyberattacker Risk Type
To determine the risk from each type of cyberattacker, look at:
Motivation
Capability
Assets of interest
Vulnerabilities to exploit
Likelihood of attempt
Likelihood of success
Existing controls
Consequences

Nation-states use their intelligence agencies and military organizations to effect cyberattacks. North Korea and Russia are labeled cyber bad guys by western media.[21] Ironically, it is getting harder to tell the bad guys from the good guys, given the global wave of ransomware attacks in early 2017 as a result of US National Security Agency (NSA) leaked cyberattack tools and hoarded vulnerabilities.

How Attacks Occur

The number of vulnerabilities detected in 2016 was 17,147, discovered in 2,136 applications from 246 vendors.[22]

Within hours of release from the vendor, cybercriminals analyze vulnerability announcements and reverse engineer security patches to discover the mechanics of the vulnerability and then weaponize a malware variant to compromise relevant applications, operating systems or mobile devices (primarily Android).

The top four cyberthreats in 2016 were malware, web-based attacks, web application attacks and DoS attacks. These attacks are successful because cyberattackers invest significant amounts from their profits to advance and mature their infrastructures.[23]

Malware is used by most cyberattacker types. All cyberattackers, except insiders, use botnets for web-based, web application and DoS attacks. All cyberattackers, except the less sophisticated script kiddies, use phishing as an attack method.[24] The primary attack vector available to cyberattackers to exploit a vulnerability in 2016 was, again, via remote network.[25]

Overall, web attacks dropped more than 30 percent between 2015 and 2016. This drop can be explained by attackers moving to email as the primary infection vector. Email is an easier way for attackers to distribute malware and is also more reliable. Exploit kits require maintenance of a backend infrastructure and are more work for attackers than sending emails. The sheer scale of email malware operations indicates that attackers are making considerable profits from these kinds of attacks and email is likely to continue to be one of the main avenues of attack in 2017.[26]

> “A CYBERATTACKER WILL COMPROMISE ANY APPLICATION OR IT SYSTEM TO GAIN A FOOTHOLD IN THE IT ENVIRONMENT, THEN MOVE LATERALLY, COMPROMISING OTHER SYSTEMS AND APPLICATIONS.”

There are no trivial systems in the organization’s IT environment. A cyberattacker will compromise any application or IT system to gain a foothold in the IT environment, then move laterally, compromising other systems and applications. One of the first objectives of a cyberattacker once in the organization’s environment is to compromise passwords. Eighty-one percent of the confirmed worldwide data breaches Verizon analyzed for its data breach investigations report involved the use of weak, default or stolen passwords.[27]

Cyberattack Trends in 2016

The following list amalgamates some interesting facts and figures from recently released cybersecurity threat reports:

- More than 4 billion records were leaked in 2016, more than the combined total from the two previous years.[28]

- Email remained the top vector for malware with the volume of malicious document attachments increasing more than 600 percent in 2016 over 2015.[29]
- Sixty-six percent of malware was installed via malicious email attachments.[30]
- Total malware has increased every quarter for the past eight quarters.[31]
- Ransomware spiked 752 percent in new families in 2016.[32]
- Ransomware distribution increased by 267 percent between June and November 2016.[33]
- Sixty percent of Australian organizations stated that they experienced at least one ransomware incident in the last 12 months.[34]
- Seventy-seven percent of all detected ransomware was in four industries: business and professional services (28 percent), government (19 percent), healthcare (15 percent), and retail (15 percent).[35]
- Adobe Flash Player, Microsoft Office and Internet Explorer exploits are still popular among cybercriminals.[36]
- The US federal government reports forty-two percent of senior IT managers from US federal agencies have experienced a data breach within the past six months and a staggering one in eight has experienced a data breach within the past 30 days.[37]
- Government institutions, followed by IT companies, financial services companies and educational institutions report the highest average number of attacks per day.[38]
- The number one programming language exploited is PHP with the associated assumption that most targets are running out-of-date Linux/Apache/MySQL/PHP installations.[39]
- Seventy-six percent of scanned websites have vulnerabilities.[40]
- Thirty-two percent of user computers were subjected to at least one malware-class web attack in 2016.[41]

These facts and figures should serve as a wake-up call to companies of all sizes and in all industries. No public or private organization or government agency is immune to cyberattacks.

From Problem to Solution

Now that the cybersecurity problem is better understood, cyberrisk management can be discussed.

After the 1984 Irish Republican Army (IRA) bombing at the Grand Hotel in Brighton, England, targeting the British cabinet, the IRA issued a statement saying, "We only have to be lucky once. You will have to be lucky always."[42]

Why is it that some companies are cyberattacked and others in the same industry are not? Luck indeed plays a part. Since no one is lucky always and forever, this means sooner or later, compromise is inevitable for everyone because everyone is a target in cyberspace, certainly by chance, and other times as a direct target.

In one survey, when asked how likely it is that the enterprise will experience a cyberattack in 2017, 80 percent of cybersecurity professionals replied "very likely" or "likely."[43] And 61 percent of global CEOs list cyberthreats in the top 10 threats facing their businesses.[44]

Cyberrisk management is different from managing other market, credit or operational risk. That is because there are cybercriminals around the world supported by a vast underground black market.

Effective cyberrisk management, then, requires thinking differently about managing this unique enterprise risk.

Executive and Board Awareness

In the past 25 years, the nature of corporate asset value has changed significantly, shifting away from the physical and toward the virtual. Nearly 90 percent of the total value of the Fortune 500 now consists of intellectual property (IP) and other intangibles.[45] Along with the rapidly expanding digitization of corporate assets, there has been a corresponding digitization of corporate risk. Accordingly, policy makers, regulators, shareholders and the public are more attuned to corporate cybersecurity risk than ever before.[46]

Cyberrisk is uniting the business community, regulators and governments alike. Pooling knowledge and openly sharing experiences can deliver valuable insights that benefit organizations of all sizes and in all industries. Not only does cyberrisk need a united effort externally, it also requires an enterprisewide approach with leadership by the top levels of management. Cyberrisk demands attention across all levels and functions. It affects everybody, from the boardroom to senior management, and from the branch office to the engine room of the business.[47]

Leadership is the single most important factor in cybersecurity protection.

A senior executive should lead the cybersecurity program to ensure management and the board truly understand the current cyberrisk state and the most critical business processes, IT systems and information assets. Only then can effective protection strategies and tactics for people, processes and technologies be developed across the whole organization.

Delegating cybersecurity solely to the IT department is where many executives misjudge the problem. When CEOs, chief information officers (CIOs) and chief information systems officers (CISOs) are fired after a cyberbreach, it is clearly not an IT problem. It is a corporate governance problem realized through the failure in the management of enterprise risk.

Enterprise cyberrisk management needs to be led from the executive suite with oversight from the board. Cybersecurity protection must be comprehensive across an organization—people, processes and technologies, with cyberrisk management accountability from the board down to every staff member.

Cybersecurity Talent

Every day another organization is being hacked. Attacks outpace defense, and one reason for this is the lack of an adequate cybersecurity workforce. The cybersecurity workforce shortfall remains a critical vulnerability for organizations and nations. Unfortunately, the main problem of obtaining key cybersecurity talent stems from a lack of qualified applicants. On average, 59 percent of enterprises get at least five applicants for each open cybersecurity position, but most of these applicants are unqualified.[48] The deficit of cybersecurity talent is a challenge for every industry sector. The lack of trained personnel exacerbates the already difficult task of managing cybersecurity risk.[49]

> “NOT ONLY DOES CYBERRISK NEED A UNITED EFFORT EXTERNALLY, IT ALSO REQUIRES AN ENTERPRISEWIDE APPROACH WITH LEADERSHIP BY THE TOP LEVELS OF MANAGEMENT.”

The struggle to find talent is a concern, considering the expertise and decision-making abilities needed to fight targeted attacks and shifting adversary tactics. A well-resourced and expert IT security team paired with the right tools can make technology and policies work together and achieve better security outcomes.[50] For companies with capital to spend, there is a plethora of security tools available in the marketplace. The challenge, then, is finding adequately skilled human resources. When asked which skill is expected to be most difficult to fill by hiring, 25 percent of technology managers and executives surveyed said security.[51]

Universities are scrambling to educate and train the emerging cyberworkforce. Among US universities offering programs in cybersecurity are Carnegie Mellon University (Pittsburgh, Pennsylvania, USA), Stanford University (California, USA), University of Texas at San Antonio (USA), University of Southern California (Los Angeles, USA), Northeastern University (Boston, Massachusetts, USA), Iowa State University (Ames, Iowa, USA), Johns Hopkins University (Baltimore, Maryland, USA) and the University of South Florida (Tampa, USA).

Cybersecurity as a Counterintelligence Function

Situational awareness is being aware of one's surroundings and identifying potential threats and dangerous situations. It is a fundamental building block in collective security and is more of a mind-set than a hard skill.

Developing situational awareness in light of today's cyberthreat landscape requires one to start viewing cybersecurity protection more like a counterintelligence function. This new way of thinking about the cybersecurity problem should compel organizations to operationalize defensive measures such as identifying and prioritizing information assets and the systems that store and transmit critical information, developing mitigation strategies and tactics, exercising response plans, creating separate highly protected networks for mission-critical information assets, and developing an end-to-end view of network and system activity to improve situational awareness.

There are three forms of threat intelligence:[52]

1. **Tactical intelligence**—Is the information gathered by security systems, scanners and sensors. Most of this is automated. From a preventive standpoint, the information gathered by these systems is often an indicator of compromise, useful for forensic work and remediation efforts, but not detailed or shared quickly enough to protect the entire organization.
2. **Operational intelligence**—Encompasses the critical components for establishing context. Currently, too much of this activity is manual, often taking too long to prevent an infiltration or breach. Big data analytics, machine learning and other automated decision-making techniques are being applied to this problem to augment human capacity and judgment with the goal of reducing response times and increasing the effectiveness of threat detection and correction.
3. **Strategic intelligence**—Is processed information that informs security policy and planning activities at the organizational level. This includes elements such as the most likely adversaries and their targets, risk probabilities and impact assessments, and regulatory or legal obligations. The net effect is an overall framework of the current cyberthreat environment, enhanced by contextual information about specific attacks and threats.

Just as traditional intelligence ascertains an understanding of adversaries' capabilities, actions and intent, the same values carry over to the cyberdomain. Cybercounterintelligence seeks to understand and characterize things such as:

- What sort of attack actions have occurred and are likely to occur?
- How can these actions be detected and recognized?
- How can cyberattacks be effectively mitigated?
- Who are the relevant threat actors in the industry?
- What assets are cyberattackers after?
- What are current cyberattacker capabilities in the form of tactics and techniques they have leveraged over time and are likely to leverage in the future?
- What sort of vulnerabilities, misconfigurations or weaknesses are cyberattackers likely to target?[53]

> "DEVELOPING SITUATIONAL AWARENESS IN LIGHT OF TODAY'S CYBERTHREAT LANDSCAPE REQUIRES ONE TO START VIEWING CYBERSECURITY PROTECTION MORE LIKE A COUNTERINTELLIGENCE FUNCTION."

Cybercounterintelligence analysis strives to better position cyberdefenses to prevent or quickly contain cyberintrusions that occur. Cybercounterintelligence analysis is aided by the attack life cycle model built upon the kill-chain framework.[54] In military parlance, a kill chain is a phase-based model that describes the stages of an attack and informs ways to prevent such attacks.

The cyber kill chain is a simple way of looking at a cyberintrusion from the perspective of the cyberattacker. To compromise a target system, an attacker follows a defined methodology as indicated in **figure 6**.[55] Ideally, the earlier in the kill chain an attack can be stopped, the better chance there is of stopping the attack.

In a cyberattack, the kill chain defense leverages the fact that a successful attack must complete all stages from planning and malware introduction to expansion and one or more command-and-control phases until the target is identified, manipulated and exfiltrated. The goal of a kill chain defense is to break one or more stages in the attack chain to stop the progress of the attack and force the opponent to start over.

Kill chain analysis makes it more effective for organizations to implement appropriate defensive controls at each stage of the attack life cycle. Clearly, the best way to protect the organization's most critical information assets and systems is to develop a defense-in-depth strategy with multiple layers of security protection through a well-constructed IT security architecture.

The Necessity of an IT Security Architecture

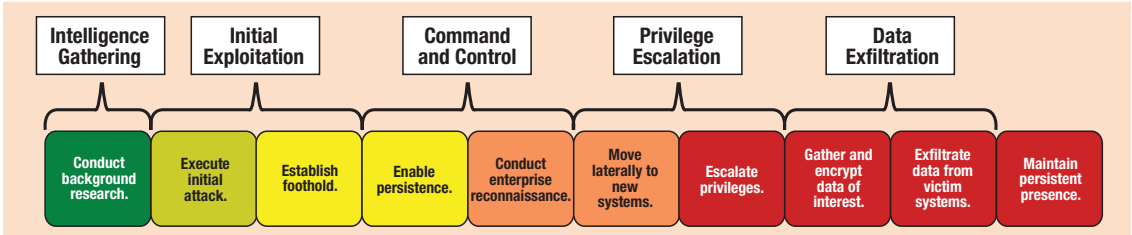
Current cyberattack scenarios should be shifting organizational security environments away from the fortress model of security strategies that are perimeter-based with disparate security controls operating independently. To combat today's cyberthreats, the security architecture overlaying the organization's IT architecture must be based on strategies such as least privilege, defense in depth, diversity of defense, choke point, systems segmentation and dedicated functionality, among others. The security architecture must include concentric layers of protection that provide multiple, diverse and complex protection barriers that an attacker (or automated malware) must penetrate one at a time. This dramatically increases the difficulty of exploitation and the time it takes, giving businesses an increased opportunity to detect and respond to attack activity.

> "THE SECURITY ARCHITECTURE MUST INCLUDE CONCENTRIC LAYERS OF PROTECTION THAT PROVIDE MULTIPLE, DIVERSE AND COMPLEX PROTECTION BARRIERS THAT AN ATTACKER (OR AUTOMATED MALWARE) MUST PENETRATE ONE AT A TIME."

Despite the increasing number of data breaches and the billions of data records worldwide that were lost or stolen in 2016, the vast majority of IT professionals still believe perimeter security is effective at keeping unauthorized users out of their networks. Many businesses are continuing to prioritize perimeter security without realizing it is largely ineffective against sophisticated cyberattacks.[56]

Enterprise networks are composed of users, devices and systems with varying security requirements with regard to confidentiality, integrity, availability, authenticity and nonrepudiation. Because the risk that faces users, devices and systems is different, it is logical to separate higher-risk entities from lower-risk entities and group like entities requiring common protection strategies. Like entities can then be grouped into zones that are collections of users, devices and systems with a similar level of trust

Figure 6—The Cyber Kill Chain



Source: Ernst & Young *Responding to Targeted Cyberattacks*, ISACA, USA, 2013. Reprinted with permission.

or those requiring similar protection and controls, logically bound together.

Trust in information technology and the confidence the organization has in it to meet its confidentiality, integrity and availability requirements is a primary security architecture objective.

Trust modeling is the process used to define a complementary threat profile and trust model based on a use-case-driven data flow analysis. The result of the analysis integrates information about the threats, vulnerabilities and risk of a particular information technology architecture. Further, trust modeling identifies the specific mechanisms that are necessary to respond to a specific threat profile.

Zero-trust modeling is an approach to information security that takes into account the possibility of threats coming from internal and external sources and protects the organization from both types of threats. Today, cybersecurity protection must fully integrate with the organization's network because the organization must contend with malicious insiders or compromised user credentials.

The real benefit of introducing a security architecture results from the gradations of protection against the volume, variety and velocity of cybersecurity threats facing the typical organization. Security zone modeling employs concentric layers of protection to dramatically increase the difficulty of exploitation. A properly constructed zoned security architecture provides formidable challenges to the cyberattacker because of protection complexity. It should increase the time required for the attacker to penetrate multiple layers and, in turn, increase the opportunity to detect attack activity.

Establish a Cybersecurity Protection Framework

A comprehensive cybersecurity assessment led by senior management is a critical first step to identify gaps in the organization's cybersecurity capability and the practical steps needed to improve protection of data and systems and respond and recover from a cyberattack incident.

The starting point for the organization's (now required) cybersecurity improvement road map should be a current-state assessment based on a formal cybersecurity assessment framework. One widely recognized approach is the US NIST Cybersecurity Framework (NIST CSF).[57] Further controls from other control libraries such as Center for Internet Security's Critical Security Controls,[58] Australian Government's Essential Eight and Information Security Manual,[59] and ISACA's COBIT® 5[60] can enhance the assessment baseline of controls.

The risk-based NIST CFS provides a set of industry standards and best practices to help manage cybersecurity risk. The framework focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risk as part of the risk management processes.

> "PROPERLY CONSTRUCTED ZONED SECURITY ARCHITECTURE PROVIDES FORMIDABLE CHALLENGES TO THE CYBERATTACKER BECAUSE OF PROTECTION COMPLEXITY."

The NIST CSF enables most organizations—regardless of current degree of cybersecurity risk or cybersecurity maturity—to apply the principles and best practices of risk management, improving the security and resilience of its business-critical infrastructure.

The framework core provides a set of cybersecurity activities and desired outcomes that are common across industry sectors for cybersecurity risk management. It presents industry standards, guidelines and practices in a manner that allows for communication of cybersecurity activities and outcomes from the executive level to the implementation/operations level.

The framework core consists of the following five concurrent and continuous functions:

1. Identifying information assets and support functions to manage cybersecurity risk to data, systems and service capabilities
2. Protecting information and systems through appropriate safeguards to ensure delivery of critical infrastructure services

3. Detecting the occurrence of a cybersecurity event
4. Responding decisively to a detected cybersecurity event
5. Recovering quickly to maintain resilience and restore the services impaired by a cybersecurity event

When considered together, these functions provide a high-level, strategic view of the life cycle of management of cybersecurity risk.

Conclusion

Given the pervasive nature of cyberattacks, it is not possible to protect everything. Security teams have to focus on protecting the organization's most critical information and systems. That changes the definition of successful defense from "keeping cyberattackers out" to "sometimes, cyberattackers are going to get in."

Understanding the cyber kill chain and how a zoned security architecture based on concentric layers of protection can help break the cyberattack chain provides a new approach to security defense. Together with a risk-based, prioritized road map for protection improvements based on an established cybersecurity assessment framework, these strategies will help the organization attain its desired future state of cybersecurity protection.

Indeed, significant challenges to effective cybersecurity protection remain. In achieving cybersecurity protection objectives, it is important to focus on bigger-picture business processes rather than just the three pillars of confidentiality, integrity and availability. Business process assurance is the ultimate objective of information, IT and cybersecurity.

This article opened with a cybersecurity reality check in **figure 1**. The article closes with the following axioms with regard to the state of cybersecurity as 2018 begins:

- Accept that the organization is a target because every organization is a target.
- Accept that there are no trivial systems in the network. Attackers will exploit any opening to break in, then move laterally, compromising other systems and applications.
- Accept that it is not possible to protect everything. Identify and protect the most critical information and systems.
- Accept that cyberattackers and malware are going to get in. Advise management to focus resources on detecting and responding to attacks as early as possible to minimize the damage.
- Protect the rest of the network from compromised desktops, laptops and Internet-facing web services by segmenting the network into security zones.
- Offense informs defense. Use knowledge of actual attacks to continually improve cyberdefenses.

> "ACCEPT THAT THE ORGANIZATION IS A TARGET BECAUSE EVERY ORGANIZATION IS A TARGET."

Endnotes

1 Cybersecurity Ventures Editors, "Cybercrime Report," Cybersecurity Ventures, 16 October 2017, *https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/*
2 Symantec, "2017 Internet Security Threat Report," 2017, *https://www.symantec.com/security-center/threat-report*
3 Businessdictionary.com, "Information," *www.businessdictionary.com/definition/information.html*
4 International Organization for Standardization, ISO/IEC 27000:2016, *https://www.iso.org/standard/66435.html*
5 International Organization for Standardization, ISO/IEC 27032:2012, *https://www.iso.org/standard/44375.html*
6 First, "Common Vulnerability Scoring System SIG," *https://www.first.org/cvss*
7 Morgan, S.; "IBM's CEO on Hackers: 'Cyber Crime Is the Greatest Threat to Every Company in the World,'" *Forbes*, 24 November 2015, *https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world&refURL=&referrer*

8 Aon, *2017 Global Risk Management Survey*, 2017, *www.aon.com/2017-global-risk-management-survey/index.html*
9 World Economic Forum, "Global Risks Report 2016," 2016, *https://www.weforum.org/reports/the-global-risks-report-2016*
10 Identity Theft Resource Center, *https://www.idtheftcenter.org/*
11 Trend Micro, "TrendLabs 2016 Security Roundup: A Record Year for Enterprise Threats," 2016, *https://documents.trendmicro.com/assets/rpt/rpt-2016-annual-security-roundup-a-record-year-for-enterprise-threats.pdf*
12 Newman, L. H.; "Yahoo's 2013 Email Hack Actually Compromised Three Billion Accounts," *Wired*, 3 October 2017, *https://www.wired.com/story/yahoo-breach-three-billion-accounts/*
13 Equifax, "Equifax Announces Cybersecurity Incident Involving Consumer Information," 7 September 2017, *https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628*
14 European Union Agency for Network and Information Security (ENISA), *ENISA Threat Landscape Report 2016*, 8 February 2017, *https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016*
15 Gemalto, "Breach Level Index 2016," 28 March 2017, *https://www6.gemalto.com/breach-level-index-report-full-2016-press-release*
16 Mandiant, "M-Trends 2017," FireEye, 2017, *https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html*
17 Dtex Systems and Ponemon Institute, "2016 Costs of Insider Threats," Dtex Systems, 2016, *https://dtexsystems.com/cost-of-insider-threat/*
18 *Op cit* ENISA
19 Verizon, *2017 Data Breach Investigations Report*, 2017, *www.verizonenterprise.com/verizon-insights-lab/dbir/2017/*
20 *Ibid.*
21 Biddle, S.; "Leaked NSA Malware Threatens Windows Users Around the World," *The Intercept*, 14 April 2017, *https://theintercept.com/2017/04/14/leaked-nsa-malware-threatens-windows-users-around-the-world/*
22 Flexera, "Vulnerability Review 2017," 2017, *https://www.flexera.com/enterprise/resources/research/vulnerability-review/*
23 *Op cit* ENISA
24 *Ibid.*
25 *Op cit* Flexera
26 *Op cit* Symantec
27 *Op cit* Verizon
28 IBM, "2017 IBM X-Force Threat Intelligence Index," 2017, *https://www.ibm.com/security/data-breach/threat-intelligence*
29 CDW, "Proofpoint Quarterly Threat Summary: Q4 2016 and Year in Review," 2016, *https://www.cdw.com/content/dam/CDW/resources/brands/proofpoint/Proofpoint-Q416-Threat-Report.pdf*
30 *Op cit* Verizon
31 McAfee, *McAfee Labs Threats Report*, 2017
32 *Op cit* Trend Micro
33 Malwarebytes, "State of Malware 2017," 2017, *https://www.malwarebytes.com/pdf/infographics/stateofmalwareinfographic.pdf*
34 Telstra Global, "Telstra Cyber Security Report 2017," 2017, *https://www.telstraglobal.com/images/assets/insights/resources/Telstra_Cyber_Security_Report_2017_-_Whitepaper.pdf*
35 NTT Communications, "Global Threat Intelligence Report 2017," 2017, *http://info.us.ntt.com/Global-Threat-Intelligence-Report-2017.html*
36 Kaspersky Lab, "Kaspersky Security Bulletin 2016," Kaspersky, 8 December 2016, *https://kasperskycontenthub.com/securelist/files/2016/12/KASPERSKY_SECURITY_BULLETIN_2016.pdf*
37 BeyondTrust, "Federal Cybersecurity Threat Survey Report," *https://www.beyondtrust.com/resources/white-paper/federal-cybersecurity-threat-survey-report/*
38 Positive Technologies, "Web Application Attack Statistics: Q1 2017," 2017, *https://www.ptsecurity.com/upload/corporate/ww-en/analytics/WebApp-Attacks-2017-eng.pdf*
39 Ixia, "Security Report 2017," 13 March 2017, *https://www.ixiacom.com/resources/security-report-2017*
40 *Op cit* Symantec
41 *Op cit* Kapersky Labs

42 BBC, On This Day, Witness, *http://newsbbc.co.uk/onthisday/hi/witness/october/12/newsid_3665000/3665388.stm*
43 ISACA, *State of Cybersecurity 2017*, May 2017, *www.isaca.org/Knowledge-Center/Research/Documents/state-of-cybersecurity-2017-part-2_res_eng_0517.pdf*
44 PricewaterhouseCoopers, "20th CEO Survey," 2017, *https://www.pwc.com/gx/en/ceo-survey/2017/pwc-ceo-20th-survey-report-2017.pdf*
45 Ocean Tomo, "Annual Study of Intangible Asset Market Value," 5 March 2015, *www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/*
46 National Association of Corporate Directors (NACD), "Cyber-Risk Oversight: Director's Handbook Series," 2017, *https://www.nacdonline.org/files/FileDownloads/NACD%20Cyber-Risk%20Oversight%20Handbook%202017.pdf*
47 ASX, "ASX 100 Cyber Health Check Report," April 2017, *www.asx.com.au/documents/investor-relations/ASX-100-Cyber-Health-Check-Report.pdf*
48 *Op cit* ISACA
49 Intel Security, "Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills," Intel Corporation, 11 July 2016, *https://newsroom.intel.com/wp-content/uploads/sites/11/2016/07/Hacking-the-Skills-Shortage-Executive-Summary.pdf*
50 Cisco, *Cisco 2017 Annual Cybersecurity Report, 2017*, *http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017*
51 Computerworld Staff, "Tech Forecast 2017: Complete Survey Results," *Computerworld*, 2017, *https://www.computerworld.com/resources/122905/tech-forecast-2017-complete-survey-results*
52 *Op cit* McAfee
53 Mitre, "Cybersecurity," *www.mitre.org/work/cybersecurity/pdf/stix.pdf*
54 Hutchins, E. M.; M. Cloppert; R. Amin; "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corp., *www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf*
55 Ernst & Young, *Responding to Targeted Cyberattacks*, ISACA, USA, 2013, *http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Responding-to-Targeted-Cyberattacks.aspx*
56 Data Security Confidence Index, *2017 Data Security Confidence Index Report*, Gemalto, July 2017, *https://www2.gemalto.com/data-security-confidence-index/*
57 National Institute of Standards and Technology, Cybersecurity Framework, USA, *https://www.nist.gov/cybersecurity-framework*
58 Center for Internet Security, CIS Controls, *https://www.cisecurity.org/controls/*
59 Australian Government Department of Defence, "Strategies to Mitigate Cyber Security Incidents," Australia, *https://www.asd.gov.au/infosec/mitigationstrategies*
60 ISACA, "What Is COBIT 5?", *www.isaca.org/COBIT/*