Feature

Effective Cyberthreat Management Evolution and Beyond

Seemant Sehgal, CISA, CISM, BS7799 LI, CCNA, CEH, CIW Security Analyst, SABSA, heads the security assessment services department at ING Bank, The Netherlands. He has engaged with organizations such as Capital One Bank, IBM, COMODO Security Solutions and Cisco Systems in various domains of information security.

Over the past few decades, cybersecurity has gained pivotal importance in the way businesses operate and survive in their value systems. Exponential growth in the number of users and devices connected to the Internet has led to an unprecedented expansion in the attack surface available to perpetrators in the world of cybercrime.

While attack vectors get more and more sophisticated, enterprises across the globe are confronted with a challenge to address their security concerns in an effective, yet cost-efficient way. Information security is possibly one of the most vibrant areas in the IT sector, in which technical innovation constantly paves the way to defeat emerging threats. This is not surprising, as the threat landscape itself is constantly evolving and it demands a constant revival of defense tactics.

Technology, however, is just one facet of defense strategy for any enterprise. A holistic view on people, process and technology is required in any organization to make the defense strategy successful. Ironically, the sheer size, complexity and geopolitical diversity of a modern-day enterprise acts as an inherent obstacle for its pursuit to achieve business objectives in a secured environment.

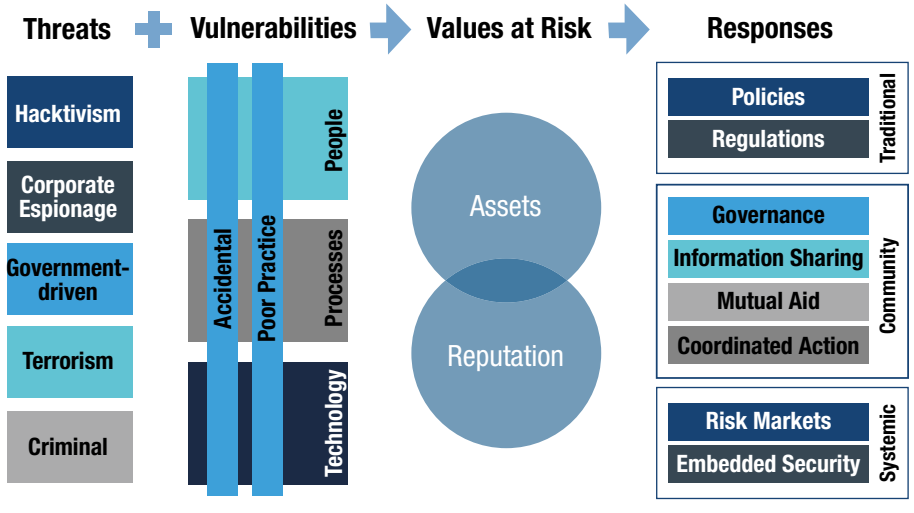
This article explores these challenges, analyzes common frameworks available to manage these challenges and deliberates on evolving possibilities that may give chief executive officers (CEOs) the agility required to cope with the cyberthreat landscape.

UNDERSTANDING THE CORE OF THE PROBLEM

One might wonder if the information security industry really understands the problem that security professionals are trying to solve. At the crux of the issue lies the paradigm of threat, vulnerabilities and value at stake for a business. An area for improvement is to solve the problem at its source.

The source of the problem is not threats themselves, but threat agents. The term "threat agent," from the Open Web Application Security Project (OWASP), is used to indicate an individual or group that can manifest a threat. So, who are these individuals or groups of individuals at the source of the problem?

Figure 1—World Economic Forum Cyber Risk Framework



Source: World Economic Forum, *www.weforum.org/*. Reprinted with permission.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

The answer to this question is easily visible in the overview developed from a study conducted by a task force at the World Economic Forum in 2014 (**figure 1**).[1] Irrespective of the type of threat, the threat agent takes advantage of the vulnerability and exploits it in an attempt to negatively impact the value the business has at risk. The attempt to execute the threat in combination with the vulnerability is called hacking. When this attempt is successful and the threat agent is in a position to negatively impact the value at risk, it can be concluded that the vulnerability is successfully exploited. So, essentially enterprises are trying to defend against hacking and, more important, the threat agent that is the hacker. This conclusion is supported by the facts presented in the Verizon *2014 Data Breach Investigations Report*,[2] which clearly shows hacking as the activity that resulted in the greatest number of breaches in the past decade (**figure 2**). In fact, most activities in this chart can be termed as the by-product of a hacker's mind-set.

TRADITIONAL CYBERTHREAT MANAGEMENT

While there is no one-size-fits-all framework to build and run a sustainable security defense in a generic enterprise context, the framework in **figure 3** reflects a high-level representation.

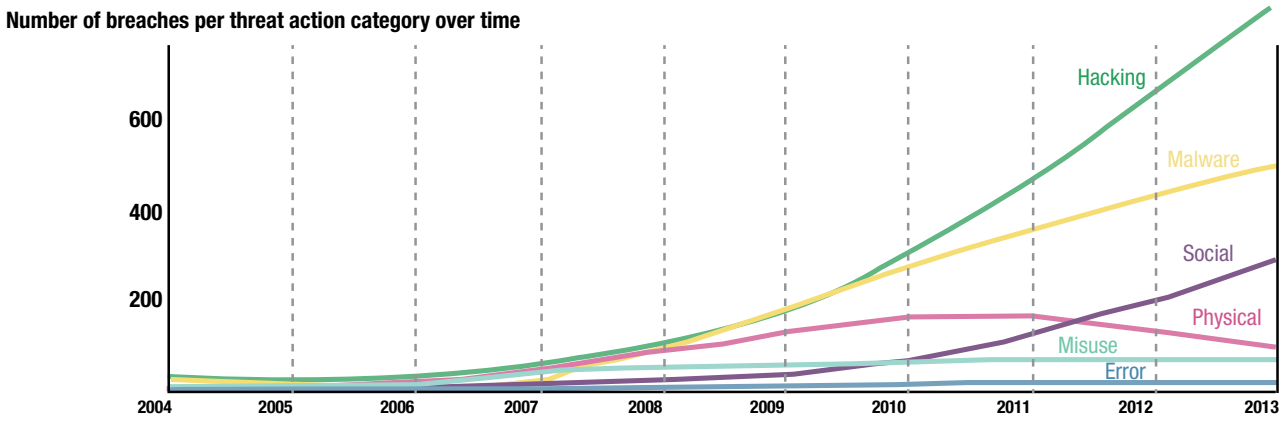
Most IT risk and security professionals would be able to identify this framework and would agree that it is a sustainable approach to managing an enterprise's security landscape. Facts prove that this is not the case. If the framework was working as intended, the number of security incidents would show a downward trend as threats would fail to manifest into incidents. They would be identified by enterprises as known security problems and dealt with in day-to-day security operations. However, recent security surveys conducted by many organizations clearly show an upward trend of rising security incidents and breaches.

The trend of rising security incidents and breaches in itself is not surprising. In 2013, 13,073 vulnerabilities were registered across vendors and technologies. That is an average of 35 new security failures each day of the year (**figure 4**).

Figure 3—IT Risk Management Framework

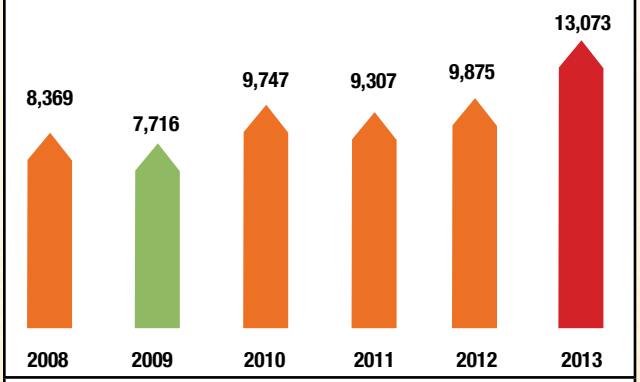
Source: Seemant Sehgal. Reprinted with permission.

Figure 2— Breaches Per Threat Action Category



Source: Verizon, *2014 Data Breach Investigations Report*, 2014, *www.verizonenterprise.com/DBIR/*. Reprinted with permission.

Figure 4—Annual Security Vulnerabilities



Source: Secunia, *www.secunia.com*. Reprinted with permission.

Couple these facts with the ease of execution and readily available exploit kits and the threat grows in both probability of exploitation and magnitude of impact. With speed and magnitude, each threat hits the security ecosystem of an enterprise and takes away its ability to deal with it in a daily operational regime. Hence, most enterprises witness a growing trend of security incidents being reported and registered.

THE EVOLVED VIEW ON ADDRESSING THE PROBLEM

Due to a sharp increase in the number of published vulnerabilities in 2013-14, many organizations had to set up emergency response teams to respond to cyberthreats and incidents. These teams are a new addition to the existing ecosystem and have two main functions: responding to security incidents and collecting internal and external security intelligence for predictive analysis.

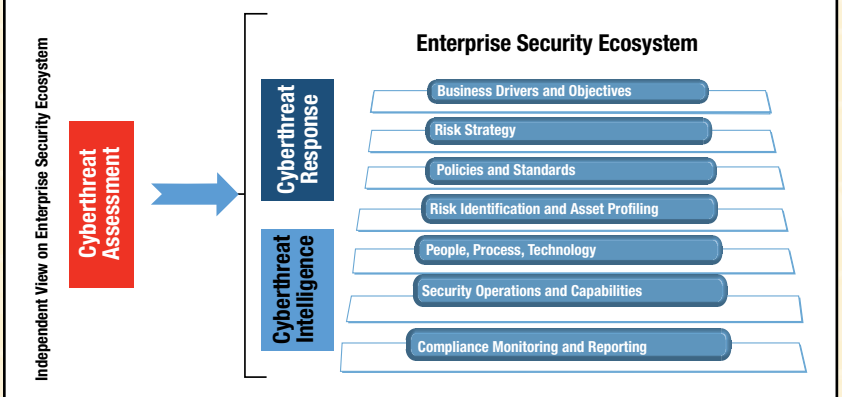
Being able to respond to security incidents via a dedicated response team boosts the capacity of the operational organization to contain and recover from the same. Responding to incidents is, in any case, a reactive approach to deal with cyberthreats. This is where cyberthreat intelligence comes into play. Threat intelligence is a more proactive means of enabling an organization to predict incidents. However, this approach also has a downside. The influx of a great deal of intelligence information may limit the prospects of making it actionable within the required time span.

Cyberthreat assessments are an effective means to add the relevance factor to this overwhelming influx of intelligence information. Cyberthreat assessment is currently recognized in the industry as red teaming, which is the practice of viewing a problem from an adversary or competitor's perspective.[3] As part of an IT security strategy, enterprises can use red teams to test the effectiveness of the security ecosystem as a whole and provide a relevance factor to the intelligence feeds on cyberthreats. This can help CEOs decide what threats are relevant and have higher exposure levels compared to others.

The evolution of cyberthreat response, cyberthreat intelligence and cyberthreat assessment (red teams) in conjunction with the existing IT risk framework is reflected in **figure 5** and can be used as an effective strategy to match the agility of evolving cyberthreats.

The cyberthreat assessment process assesses and challenges the ecosystem of enterprise security systems, including designs, operational-level controls and the overall cyberthreat response and intelligence process to ensure they are capable of defending against relevant cyberthreats.

Figure 5—Evolution of Cyberthreat Management



Source: Seemant Sehgal. Reprinted with permission.

HOW CEOS CAN ADAPT TO THE EVOLVED VIEW

While the traditional view of cyberthreat management is purely based on threat perception, the evolved view is a step ahead in terms of its relevance to the evolving threat landscape. In the past, enterprise risk and security decisions were based on theoretical risk assessment exercises only. This trend was mainly encouraged by a compliance-oriented mind-set. As cyberthreats grew in scale and complexity, the industry realized the gap between perceived threat and real threat. This led to the emergence of threat landscape monitoring and threat intelligence capabilities. Cyberthreat intelligence strengthens response capabilities by supplying the required information, which can be made actionable and help enterprises prepare for emerging threats.

Most threat intelligence solutions available in the market today are driven by external and mostly public sources of threat information. Another source of such information can be fellow organizations and competitors. The amount of data an organization receives from such shared information can be quite overwhelming. This is why it becomes important to add a relevance factor to it. This can help CEOs decide what threats are easier to combat for the threat agents and where they can afford to accommodate an evolution road map for their defense capabilities.

Cyberthreat assessment exercises can be extremely helpful to highlight the most relevant cyberthreats and quantify their potential impact. The word "adversary" in defining "red team" is a key element that emphasizes the need to independently challenge the security ecosystem from the view point of an attacker.[4] Red team exercises should be independent of the scope, asset profiling, security, and IT operations or coverage of existing security policies. Only then can enterprises bring in the attacker's perspective, measure the success of its risk strategy and see how it scores when challenged.

It is important that red team exercises look at the ecosystem as a whole and point to flaws in all components of the IT risk framework. It is a common notion that a red team exercise is a penetration test. This is not true. Use of penetration test techniques is a means to achieve the required information to replicate cyberthreats and create a controlled security incident. The technical shortfalls that are discovered as a result of this exercise are mere symptoms of gaps that may exist in the governance of people, processes and technology. Hence, to make the organization more resilient against cyberthreats, focus should be kept on addressing the root cause and not merely fixing the security flaws discovered during the exercise. Another key aspect to keep in mind is to include cyberthreat response and threat monitoring in the scope of such assessments. This demands that such exercises be executed, and partially announced, with CEO-level approval. This ensures that enterprises challenge the end-to-end capabilities of an enterprise to cope with a real-time security incident. Lessons learned can be capitalized on to improve the overall security posture of the organization.

CONCLUSION

As cyberthreats evolve, 100 percent security for an active business is impossible to achieve. Business is about making optimum use of existing resources to derive the desired value for stakeholders. Cyberdefense cannot be an exception to this rule. To achieve optimized use of security investments, CEOs should ensure that the security spending for their organization is mapped to the emerging cyberthreat landscape. Red teaming is an effective tool to challenge the *status quo* of an enterprise's security framework and derive facts about its security state. Not only can these facts be used to improve cyberthreat defense, they can also prove to be an effective mechanism to steer a higher return on cyberdefense investments.

ENDNOTES

[1] World Economic Forum, Partnering for Cyber Resilience (PCR), 2014, *www.weforum.org/issues/partnering-cyber-resilience-pcr*

[2] Verizon, *2014 Data Breach Investigations Report*, 2014, *www.verizonenterprise.com/DBIR/*

[3] Red Team Journal, "Read Team," Glossary, *http://redteamjournal.com/glossary/glossary-red-teaming/*

[4] Secunia, Vulnerability Review, 2014, *http://secunia.com/vulnerability-review/vulnerability_update_all.html*