ESG

Enterprise Strategy Group | **Getting to the bigger truth.™**

Solution Showcase

Randori: Helping Mitigate Cyber Risk by Attacking Like the Bad Guys

Date: March 2019 **Author:** Jon Oltsik, Senior Principal Analyst and ESG Fellow

Abstract: One of the biggest security challenges for today's CISOs is understanding where and how their IT systems may be attacked next. Penetration testing can be employed to support this need for identifying potential vulnerabilities, by breaking into IT systems to test an organization's defenses. Unfortunately, the value of traditional penetration testing is limited as it is often treated as a 'check-the-box' exercise to meet compliance and customer requirements, diminishing its effectiveness for reducing cyber risk. CISOs need to embrace the value and potential here by adopting the latest tactics, techniques, and procedures (TTPs) used by sophisticated cyber-adversaries. Randori can help organizations accomplish this.

Overview

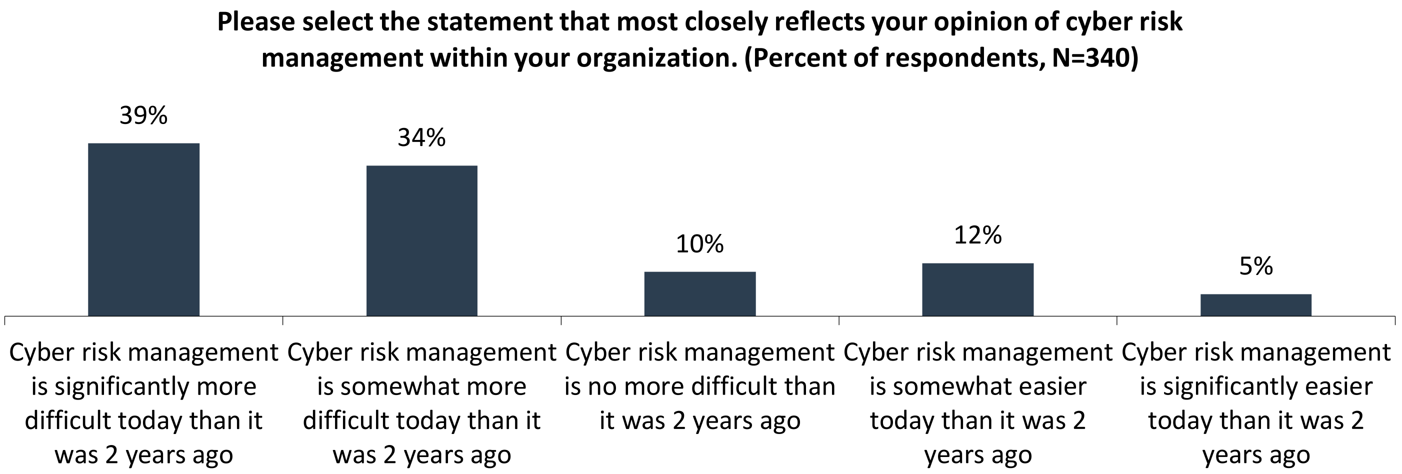
IT organizations are increasingly at risk as a result of the sheer quantity of IT systems that are unknowingly susceptible to attack due to numerous factors, including:

1. A growing number of software vulnerabilities.
2. Ever-changing and rapidly expanding attack surfaces that reflect the movement to hybrid cloud architectures.
3. IT systems that often include connections to third-party organizations.
4. An increase in the technical sophistication and pervasiveness of the threat actors.
5. The absence of real-time threat assessments, due to a lack of continuous monitoring.

It was therefore no surprise that nearly three-quarters of the 340 security professionals surveyed by ESG recently believe that cyber risk management is more difficult today than it was just two years ago (see Figure 1).[1]

[1] Source: ESG Research, Cyber Risk Management Survey, 2018. All ESG research references and charts in this solution showcase have been taken from this research.

Figure 1. Difficulty of Cyber Risk Management Compared to Two Years Ago

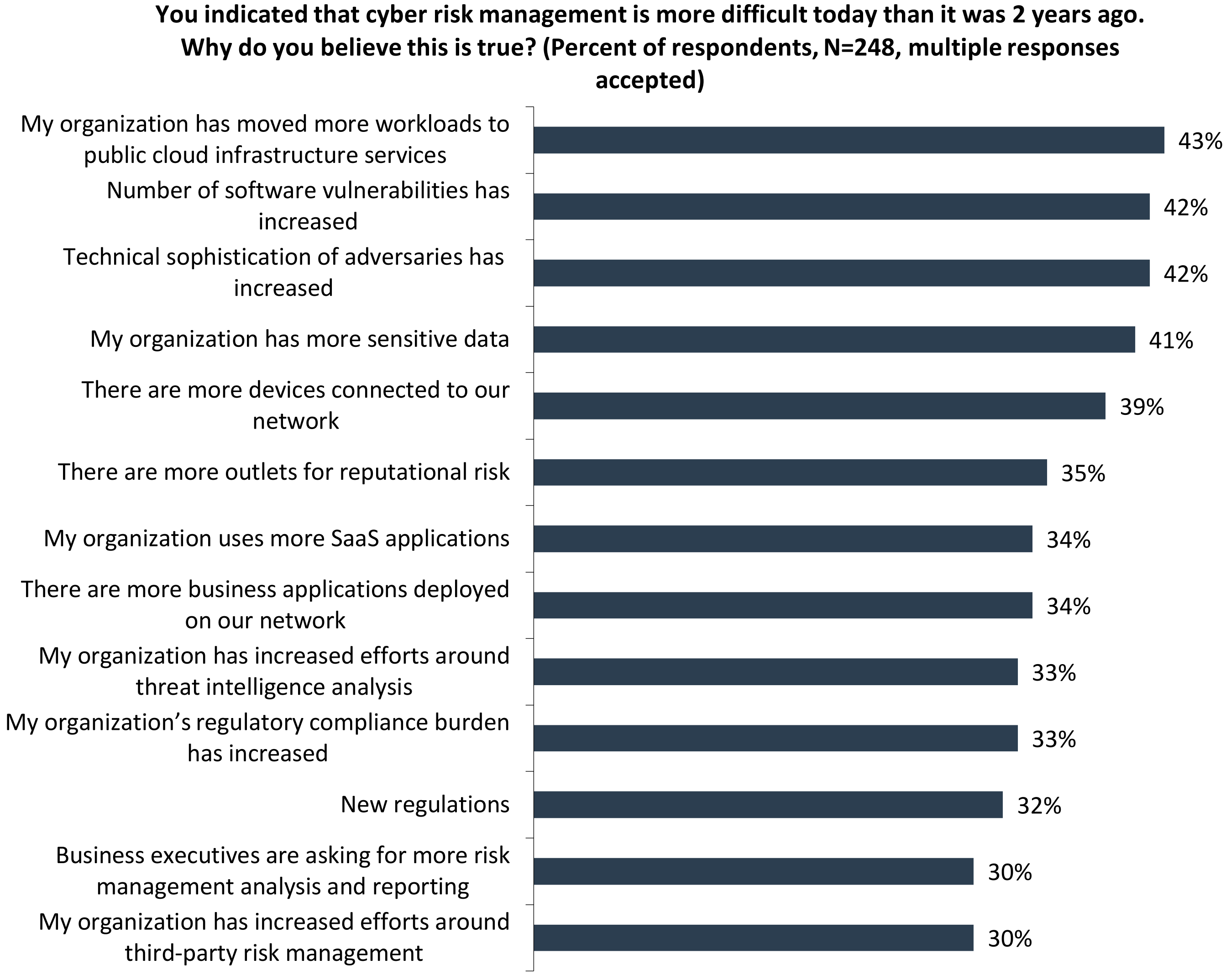


Source: Enterprise Strategy Group

Given the large number of respondents who believe that cyber risk management has gotten more difficult, ESG then asked the following question: "Why do you believe cyber risk management is significantly more difficult today?" As it turns out, there are many possible answers to this question. Reasons cited by the IT security and risk management professionals surveyed by ESG include the movement of workloads to public cloud infrastructure services in order to take advantage of the shared infrastructure and scale available, a growing amount of sensitive data from a variety of different sources, and a growing number of devices being connected to organizational networks (see Figure 2).

The research also indicates that CISOs are increasingly being asked by business executives (30%) for more risk management analysis and reporting, ostensibly so that they can better understand the implications of cyber risk to their business. This includes increased efforts (30%) in understanding the cyber risks associated with third parties. In many cases, the cybersecurity teams are challenged to deliver the frequency of updates or the level of detailed reporting that business executives desire.

Figure 2. Cyber Risk Management More Difficult for Most Organizations



Source: Enterprise Strategy Group

Underlying Issues

Historically, many organizations viewed cyber risk management as a necessary evil required to address regulatory compliance checklists or respond to corporate audits. This limited view left many firms with point-in-time risk visibility. This creates a cyber risk management gap as:

- **Organizations can't identify vulnerabilities or the types of attacks that might exploit them.** Penetration testing can be used to identify hidden vulnerabilities and risks and is one of the most direct and proactive cybersecurity activities organizations can do to assess their vulnerabilities and protect themselves from an attack. However, the benefits of penetration testing are being minimized by organizations that only conduct these exercises on a periodic basis and use tools and techniques that often do not reflect those employed by their potential attackers. In fact, the majority (75%) of penetration and/or red team exercises last only one to two weeks while threat actors operate on their own schedules.

- **Fundamental challenges make it increasingly difficult to assess the likelihood of attack and severity of impact.** Forty-seven percent of survey respondents say that monitoring risk associated with IT vendors is one of their biggest cyber risk management challenges, 44% say monitoring risk associated with shadow IT and associated devices and software misconfigurations, 41% say monitoring risks associated with third parties, and 40% say monitoring risks related to employees are among their biggest cyber risk management challenges. Combined, these challenges may help explain why respondents say that continually measuring all cyber risk across the entire IT infrastructure is one of their biggest cyber risk management challenges (46%).

- **Cyber risk management challenges are exacerbated by the global cybersecurity skills shortage.** A majority of respondents (59%) stated that their organization does not have the right skills to conduct internal penetration testing or red team exercises on their own. Add in the fact that today's threat actors are increasingly sophisticated, and target and exploit weaknesses using ever-evolving tools and techniques, and it's easy to conclude that cyber-adversaries have a distinct and growing advantage over defenders.

What's Needed?

ESG research indicates that, for many organizations, a successful cyber risk management strategy often starts with implementing a risk management framework such as the NIST cybersecurity framework (51%), or the COSO Enterprise Risk Management Framework (48%) used by many ESG survey respondents.

In addition, ESG recommends the following:

1. Penetration testing/red teaming can help bridge the cyber risk management gap by providing details about what's vulnerable and how an adversary would attack. Armed with this information, organizations can make informed and timely risk mitigation decisions.

2. The research indicates that organizations are doing penetration testing/red teaming on a periodic basis, but this doesn't work. They should strive for a methodology that incorporates penetration testing on a continuous basis.

3. Organizations should conduct continuous penetration testing based upon the latest TTPs from cyber-adversaries. In this way, they can remain in step with current threats, not just historical threats.

4. The research indicates that most organizations don't have the skills or resources to do this on their own. They should seek out skilled service providers with SaaS-based offerings that can be deployed quickly, use techniques based upon the latest TTPs, and include reports for IT and business executives.

The Attack Platform offered by Randori has the potential to support many of these requirements. The company's mission is to put the power of a red team into the hands of the CISO via an on-demand cloud-based platform that is easy to employ. It seeks to help defenders see the world through a different set of eyes, to teach them to practice the way real attackers engage and fight—rather than use off-the-shelf penetration tools or predefined scripts under controlled conditions that often don't reflect the real world. Based on its experience, Randori knows that companies who value and test their cyber defenses from an attacker's perspective are better able to understand their vulnerabilities, have smaller attack surfaces and stronger security programs, and are more effective at cyber risk management.

Randori's solution emulates the full kill chain of an attack so that security leaders can look through the eyes of the enemy while their teams experience and defend against Randori's safe but authentic attacks. It combines continuous reconnaissance, real-time target analysis, and the ability to safely execute attacks on demand to provide an attacker's perspective of where and how threat actors will strike next, making it easier to understand and validate the impact specific attacks pose to their organizations. Based upon the real-world experiences of its founders, Randori's attack platform can help CISOs gain real-time risk visibility, improve risk mitigation priorities, and work with business managers on a cohesive cyber risk management strategy.

The Bigger Truth

Cybersecurity teams often don't know where system vulnerabilities will be discovered until they find themselves under attack. However, proactive CISOs know that the best defense often starts by understanding a potential attacker's goals and methodologies and then utilizing that information to determine where the greatest vulnerabilities exist.

To more effectively manage cyber risks, organizations should incorporate an attacker's perspective into their overall cyber risk assessments to enable them to more effectively assess the likelihood of an attack. Organizations should also implement solutions that support continuous perimeter monitoring to better address new security challenges such as risks associated with shadow IT and third-party IT connections. They should also invest in capabilities or solutions that quantify impact, such as internal red teaming, more frequent penetration tests, or breach and attack simulation tools. Security leadership (CISOs/CSOs) must also be prepared to provide increasing amounts of visibility to their business leaders and board members. Moving forward, CISOs may find it worthwhile to work with SaaS-based attack platforms like Randori's to improve the timeliness and accuracy of their cyber risk management programs.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.