CyberTalk

PREVENTION:

TURNING THE TABLES ON CYBERATTACKS

Introduction

Stuxnet, WannaCry, NotPetya, Sony, Target, Equifax, Marriott, and Yahoo. The mere mention of these mega cyberattacks continues to haunt individuals and organizations. The impact has been so profound that one executive survey says cyberattacks are their top business concern.[1] However, only 11% of senior leaders expressed a high degree of confidence in their ability to assess cyber threats, prevent cyberattacks, and respond effectively.[2]

Company boards often have two misconceptions about cyber security, says Ciaran Martin, CEO of the UK's National Cyber Security Centre.[3] First, that all cyberattacks are targeted to specifically chosen companies, and second, board-level executives think cyber security is too complex, thus distancing themselves from it. Either or both of these reasons can put an organization's security posture at risk.

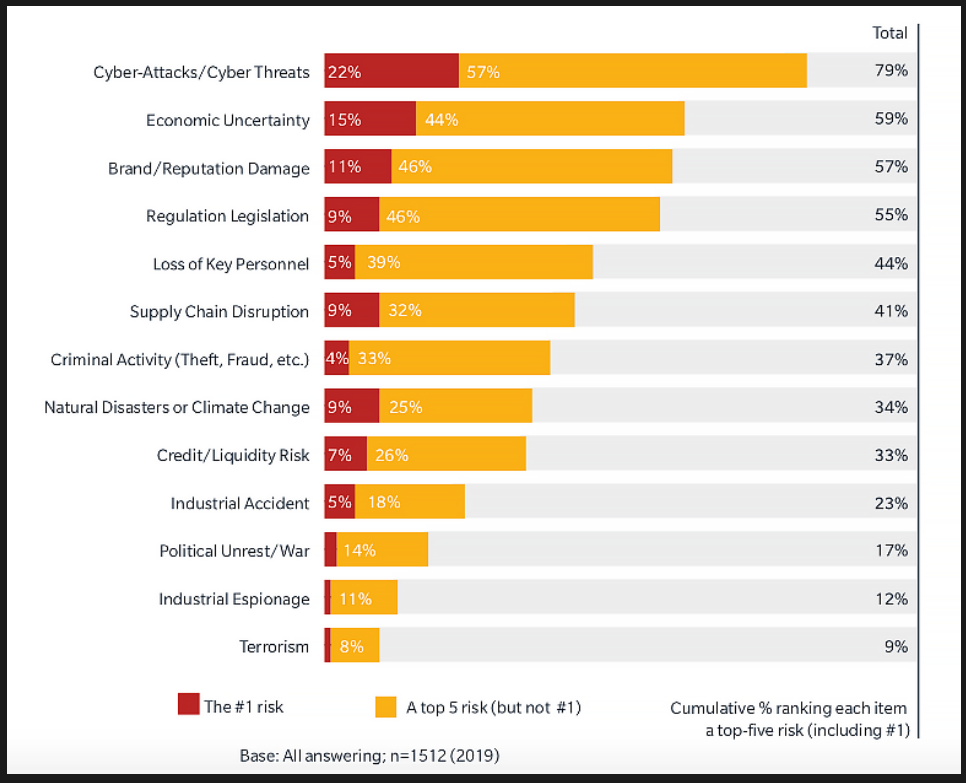

Figure 1. Source: Marsh and Microsoft – Top Business Concerns

Per the chart on the left, cyberattacks and cyber threats are outpacing other business concerns, such as economic uncertainty, brand/reputational damage, and regulation legislation.

[1] "Microsoft: Cyberattacks now the top risk, say businesses," by Liam Tung, ZDNet, September 19, 2019

[2] "How organizations view and manage cyber risk," Help Net Security, September 19, 2019

[3] "Two cybersecurity myths you need to forget right now, if you want to stop the hackers," by Danny Palmer, ZDNet, February 12, 2019

Basic Prevention Principles

The following recommendations can serve as a helpful reminder when reviewing your basic security:

1 Maintain Security Hygiene

1. **Patching:** All too often, attacks penetrate computer systems by leveraging known vulnerabilities for which a patch exists, but has not been applied. Organizations should strive to ensure up-to-date security patches are continuously maintained across all systems and software.

2. **Segmentation:** Networks need to be segmented. Apply firewall and IPS safeguards between the network segments so you can contain infections and prevent them from propagating across the entire network.

3. **Review:** Security products' policies must be carefully reviewed, and incident logs and alerts monitored continuously.

4. **Audit:** Conduct routine audits and penetration testing across all systems.

5. **Principle of least privilege:** Keep user and software privileges to a minimum. Limit local admin rights on user PCs.

6. **Plan for failure:** Make sure backup systems are maintained so IT can monitor security measures and react rapidly to a breach.

7. **Record:** If a breach does occur, the event needs to be recorded. This data can be important in analyzing an attack and can help prevent further occurrences.

8. **Testing:** For information security to keep pace with hackers, constant tests, risk assessments, updating disaster recovery and business continuity plans are required.

2 Choose Prevention Over Detection

Traditional cyber security vendors often claim that cyberattacks will happen, and that the best you can do is to detect the attack once it has already breached the network, and respond as quickly as possible. You are typically instructed to mitigate the damages immediately. However, there is another way.

Cyberattacks can be prevented, including zero-day attacks and unknown malware. With the right technologies in place, the majority of attacks, even the most advanced, can be prevented without disrupting the normal business flow.

3 Leverage a Complete Unified Architecture

Cyber security for many companies has become a patchwork of single-purpose point products from multiple vendors. This approach usually results in disjointed technologies that don't collaborate – creating security gaps. Plus, it introduces huge overhead when using multiple systems and vendors. As a result of this inefficient approach, many attacks are not prevented, forcing organizations to invest more on post-infection and breach mitigation.

In order to achieve comprehensive security, companies should adopt a unified multi-layer approach that protects all IT elements – networks, endpoint, cloud, and mobile, all sharing the same prevention architecture and the same threat intelligence.

> Over the last three years, the number of vulnerabilities in multi-cloud environmants are nearly tripling to 16,555 in 2018.

4 Cover all attack vectors

It's common knowledge that cyber criminals will exploit any and all possible entry points. Over the last three years, digital transformation has seen the rise of multi-cloud environments, smartphones, and IoT devices, and with that, the number of vulnerabilities are nearly tripling to 16,555 in 2018.[4] Be sure to secure these common attack surfaces:

---

[4] Source: CVE Details, MITRE

- **Email and messaging:** Malicious attachments and links are a hacker's tried and true method of penetrating the network.
- **Web browsing:** User's browsers can be compromised or a user can be tricked into downloading and opening a malicious file (typically through exploit kits).
- **Server and systems exploitation:** Infections caused by exploiting unpatched vulnerabilities in any online host.
- **Mobile apps:** Mobile devices are compromised through mobile apps.
- **External storage:** Physically mounted drives allow malicious files to enter without even traversing the network.
- **Phishing:** Attempts to obtain sensitive information by disguising oneself as a trusted person and/or company.

5 Implement the Most Advanced Technologies

Over the past three decades, cyberattacks have evolved to today's mega fifth generation. Unfortunately, most organizations use cyber security that protects against second or third generation threats. Advanced technologies such as AI and machine learning, behavioral analysis, sandboxing, anomaly detection, and content disarmament, among others, are proving effective in covering specific file types or attack vectors. These advanced solutions integrate a broad range of technologies and innovations in order to effectively combat modern attacks in IT environments.

6 Keep Your Threat Intelligence Up to Date

In the constant fight against malware, threat intelligence and rapid response capabilities are essential. Use comprehensive intelligence to proactively stop threats, manage security services to monitor your network, and deploy incident response to quickly respond to and resolve attacks. With your organization's financial, personal, and intellectual assets on the line, be sure to implement threat intelligence that can predict, recognize attack patterns, and send notifications across all your attack vectors.

Conclusion

Recent mega cyberattacks have significantly changed what we know about the threat landscape and what we need from cyber security technologies in this digital age. Today's outbreaks spread rapidly and without effective protection, can devastate an organization. Cyber attackers are organized, well-funded, and at times sponsored by nation-states. Cyberattacks are relentless with an organization of 1,000 users receiving 300 unknown malicious files monthly.[5]

The cyber battlefield has moved from preventing not only known attacks, but evasive never-been-seen-before unknown cyberattacks. The days of relying on post-infection breach detection and mitigation as your sole security strategy is obsolete.

In order to truly combat the next generation of threats, organizations must think proactively and use advanced technologies that can prevent even the most evasive zero-day attacks. Further, organizations should seek out a unified, multi-layered cyber protection architecture, implemented across their entire IT infrastructure and covering all attack vectors.

Check Point offers Zero-Day Protection with CloudGuard and SandBlast solutions. Sixty-four intelligent engines prevent known and unknown threats. Check Point Infinity offers a unified architecture and multi-vector control via a single console and with unified policy management. Check Point ThreatCloud is a leader in providing cyber threat intelligence with 4 billion transactions daily.

For further information, go to Check Point Infinity.

[5] Source: Check Point Research

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com

© 2020 Check Point Software Technologies Ltd. All rights reserved.