Check Point®
SOFTWARE TECHNOLOGIES LTD

CYBER SECURITY:
IT'S ALL ABOUT MANAGING YOUR RISKS

> "Nothing in life is to be feared, it is only to be understood. Now is the time to understand more so that we may fear less."
>
> - Marie Curie

In cyber security, status quo is a non-existent concept. Hyper-sophisticated cyberattacks demand the full spectrum of the latest strategies and tools. As your organization's trusted security leader, your role requires you to effectively predict, assess, and manage cyber risks.

In this white paper, discover how you can better understand the threat landscape, assess possibilities vs. probabilities, and manage your security approach. Find out how automation and custom-built tools can help you implement strong cyber security initiatives, and ultimately mitigate as much risk as possible.

Forecasting the Future: Predicting Risk

With cyber security, "The top challenge is often overlooked—it's the ability to look forward," says Matt Palmer, CISO for risk management company, Willis Towers Watson.[1] No one can predict the future, but we can prepare by examining all available evidence.

Qualitatively, you need to know about attack vectors and exploits. Industry experts devote innumerable hours to contemplating next-generation attacks, and spend countless moments on stage, radio, podcast or other forms of media to discuss new threat intelligence. Their insights allow you to understand what you need to monitor, upgrade or implement to prevent network compromises.

[1] "How to Survive in the CISO Hot-Seat," CSO Online, June 8th, 2016.

Quantitatively, risk analysis frameworks enable organizations to obtain metrics pertaining to the elements of their security systems that are exposed vs. secure. Calculating risk exposure using a framework helps organizations estimate the annual rate of threat occurrence, and also helps organizations budget appropriately. A series of risk management frameworks exist[2,3,4,5,6] including the following:

- SERA, published by Carnegie Mellon University
- COBIT 5, developed by non-profit ISACA
- OCTAVE Allegro, also developed by Carnegie Mellon University
- The Federal Financial Institutions Examination Council Cybersecurity Assessment Tool, designed specifically for financial institutions
- HealthIT.gov, a risk assessment for small-to-medium-sized healthcare organizations

After analyzing security performance metrics relative to capabilities using a framework, organizations can consider measuring cyber readiness through additional avenues, including red teaming, technical assessments, and 'wargaming.'[7] By determining your organization's risks, you will be in a better position to select risk management products and platforms to deploy.

> " The top challenge is often overlooked—
> it's the ability to look forward."
>
> - Matt Palmer, CISO, Willis Towers Watson

[2] "Introduction to the Security Engineering Risk Analysis (SERA) Framework," Carnegie Mellon University, December 2014, Christopher J. Alberts, Carol Woody, Audrey J. Dorofee

[3] "About COBIT 5," ISACA, August 10th, 2019

[4] "Introducing OCTAVE Allegro, Improving the Security Risk Management Process," Carnegie Mellon University, May 2007, Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson

[5] "Cybersecurity Assessment Tool," FFIEC, Federal Financial Institutions Examination Council, August 29th, 2019

[6] "Security Risk Assessment Tool," HealthIT.gov, July 19th, 2019

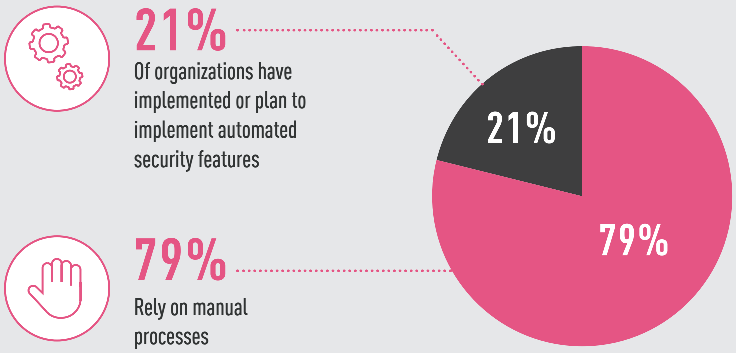
[7] "Metrics that Matter: How to Measure the Effectiveness of Corporate Security Programs," Security Magazine, August 8th, 2019

Aligning Predictions with Reality: Assessing Risk

When it comes to predictions, many organizations predict insider threats. An outstanding 90% of organizations feel vulnerable to malicious insider behavior.[8] One in five organizations encounters threats from disgruntled employees with network access.[9]

One of the most valuable ways to protect assets from insider attacks is to implement a zero trust strategy. The zero trust approach focuses on locking down assets by limiting access privileges. This multi-layered tactic is underpinned by a series of implementation principles, which include network segmentation, continuous data protection, and analyses of every user's activities.[10]

A recent Forrester study showed that organizations deploying zero trust strategies reduce risk exposure by nearly 40%, and reduce costs by a full 31%.[11] The zero trust model reinforces network security defenses, and offers a comprehensive approach to insider threats.[12]



21% Of organizations have implemented or plan to implement automated security features

79% Rely on manual processes

People just can't keep up with the constant barrage of cyberattacks. A Ponemon Institute study released in April of 2019 recorded 79% of survey respondents rely on automated security features.[13] Leveraging automated security can enhance threat detection.

[8] "Insider Threat, 2018 Report," CA Technologies, Holger Schultze

[9] "Ignore the Insider Threat at your Peril," Dark Reading, Bryan Sartin, April 8th, 2019

[10] "Absolute Zero Trust Security with Check Point Infinity," Check Point Software, 2019

[11] "Debunking 5 Myths about Zero Trust Security," Dark Reading, Torsten George, March 7th, 2019

[12] "Software Defined Protection (SDP)," Check Point Software, 2019

[13] "The Cybersecurity Automation Paradox," DarkReading, April 18th, 2019

What other automated asset can improve your risk management and threat analysis?

With a single management console, you can erase 'network complexity' from your list of risks. An automated console will enable you to eliminate point solutions, plus gain a wealth of other exciting benefits.

The use of point solutions expands attack surfaces, making your perimeter larger, and more challenging to secure. With 50 point programs running, how can you install updates, patches, and monitor vulnerabilities all at once? It's tough, and potentially invites hackers to exploit your limitations. With an automated single management system, streamlined capabilities and machine learning options can help you detect threats.

Single management consoles also offer operational efficiency and control. Your access points can be controlled all in one place. Reporting is straightforward and does not require any extra number crunching or cross-correlation of the data. With increased visibility and scalability, you're able to focus on other areas.

To oversee the aforementioned processes and systems, and to further mitigate risk, insure that you're hiring enough talent. Seventy percent of business organizations report having struggled to find qualified cyber security professionals for the past three years, while 27% of companies cannot fill vacancies.[14] The talent choices are sparse, either forcing you to attract top quality pros by offering exceedingly generous compensation packages, or to consider retraining current employees.

The talent that you need *might* already be nearby. Consider recruiting your current IT staff to learn cyber security by sponsoring professional development opportunities. Your own staff, who know the company, and can work in a cross-disciplinary fashion, might be your best choice.

> With an automated single management system, you have streamlined capabilities, and machine learning options...

[14] "How to Become a Cybersecurity Pro: A Cheat Sheet," TechRepublic, May 16th, 2019

Tailoring your Approach: Mitigating Risk

Staff who know your organization well can more easily identify needs, and do the best job of tailoring your security to correspond with business objectives. Tailored risk management protocols can address specific threats or vulnerabilities that a given organization expects to encounter.

One U.S. government agency specifically chose a customizable cyber security product because the features permitted the agency to create special notifications that alerted users to certain security situations, or certain legal compliance requirements. "With our previous product, many users weren't even aware they were out of compliance or violating agency policies," stated the group.[15] The customizable platform strengthened both internal and external security risk management capabilities.

Every business has a unique structure and a unique set of goals. With customizable management options, you can gain maximum visibility into the aspects of security that are critical for your organization. Focus on what matters.

In Conclusion:

Dodging every single cyber incident is impossible, but a well-governed cyber security strategy will enable you to manage technological risks within an acceptable margin.[16] The more you know about risks, risk management, reporting and analytics, the stronger the prevention strategies and defense mechanisms you'll put in place.

To keep business risk within acceptable bounds, an automated security solution is imperative.[17] Take advantage of increased security, reduced complexity, enhanced visibility, improved human resource management, and custom controls.

[15] "U.S. State Agency- Endpoint Security," Check Point Software, 2019

[16] "The Future of Cyber Survey 2019," Deloitte

[17] "Employees Beware: 33% of CEOs will Fire you if you Cause a Cybersecurity Breach," TechRepublic, Alison DeNisco Rayome, June 3rd, 2019

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