Balbix

CISO Primer: 5 Steps to Building Cyber-Resilience

Cyber-resilience is the ability of an enterprise to limit the impact of security incidents by deploying and arranging appropriate security tools and processes. To successfully build and enhance your organizational cyber-resilience, it is critical to understand that the role of the CISO encompasses more than just being a compliance monitor and security enforcer. The CISO must elevate security conversation to the board and instill a culture of shared cyber-risk ownership across the organization.

The following five step plan with get you on the right path to building your cyber-resilience and stay ahead of the adversaries:

1 Achieve true visibility across your entire environment

You can't protect what you can't see. The first step to cyber-resilience is to obtain a big picture view of your enterprise in terms of all the assets – devices, users, and applications – connected into your environment, and the ability to drill down into details as needed.

The IT assets that you cannot see are the ones that pose the biggest risk. And just seeing them is not enough-true visibility will come from knowing exactly how many devices – managed, unmanaged, BYO, IoT, etc. – are plugged into your environment at all times and understanding which of these assets are highly critical for your business and which ones are less important.

Read this white paper to learn more on true visibility.

2 Hire and retain top talent

Tackling organizational issues such as a shortage of security talent to support operational and technical activities is a key issue that can keep CISOs challenged. You can leverage existing talent by developing desired security skill-sets, training them with the right tools, and partner with vendors that can serve as trusted advisors.

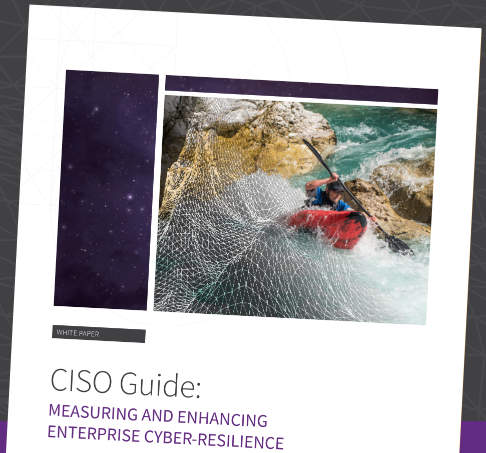
Another option is to outsource the security function to managed security service providers (MSSPs) and utilize intelligent Security Operations Centers (SOCs).

Read this blog post on the characteristics of an Intelligent SOC.

3 Elevate cybersecurity to be a board-level issue

Educate your board of directors about cybersecurity and get their buy-in. Inform them regularly about how the actions of the security team enable business initiatives and how they tie into the goals of the company. It is also important to avoid getting into technical KPIs and rather, talk about metrics around risk, such as mean time-to-failure. Leverage true visibility discussed above to connect the dots between the actual truth on the ground and the organizational security posture.

Check out this white paper or more information.



WHITE PAPER

CISO Guide:

MEASURING AND ENHANCING ENTERPRISE CYBER-RESILIENCE

4 Develop laser-focus on security fundamentals

Organizations cannot protect themselves at all times from the myriad of potential attacks through multiple channels. So, putting in place structures, technologies and processes to build cyber-resilience is critical to operating effectively in today's hyper-connected world. However, the difficulty in differentiating between what is critical and what's less important can lead to the deployment of a plethora of tools and controls, without first understanding whether they work well and in tandem with one another, or whether they are indeed holistically effective. In such circumstances, going back to first principles and really starting with the security fundamentals can be useful.

Read this paper to understand our 3-step approach to avoiding breaches.

5 Get proactive to avoid breaches

In the current sophisticated threat environment, traditional security tactics, which are mostly reactive blocking and remediation, are inadequate. The conventional wisdom of identifying and adding more point products to the tool mix has become less effective than ever. Overwhelmed and understaffed security teams are routinely challenged to simultaneously sift through alerts, track vulnerabilities, apply security policies across various systems and endpoints, and accurately assess global threat data to figure out how it can affect them in real time.

To manage these competing challenges, organizations must evolve their security posture from a purely defensive and reactive stance focused on malware to a more proactive approach of predicting and proactively mitigating breaches , which will improve both cyber-resilience and security team productivity.

Learn more about shifting your perspective from remediating to avoiding breaches in this paper.

WHITE PAPER

Shifting Perspective:

FROM REMEDIATING TO AVOIDING BREACHES

Balbix

Balbix

3031 Tisch Way, St 800
San Jose, CA 95128
866.936.3180

info@balbix.com
www.balbix.com