Elevate Security

A CISO's Guide

Maximizing Security and Enabling Business Efficiency

While security challenges are different across organizations, all CISOs are required to protect their organization from threats and minimize risk while allowing employees to do their jobs without significant friction.

Although this presents great challenges, CISOs do not have to choose between security and business efficiency, rather, with the right approach, **security leaders can reduce cyber incidents and increase their resilience while driving business performance**. By identifying which employees are most likely to fall victim to various attack vectors, security leaders can enable better outcomes with **adaptive security** – increasing or decreasing security controls based on the type of risk an employee poses to the organization.

Here is how to achieve this in practice:

I. Understand How Employee Security Decisions Impact Risk

II. Identify Areas of Greatest Risk

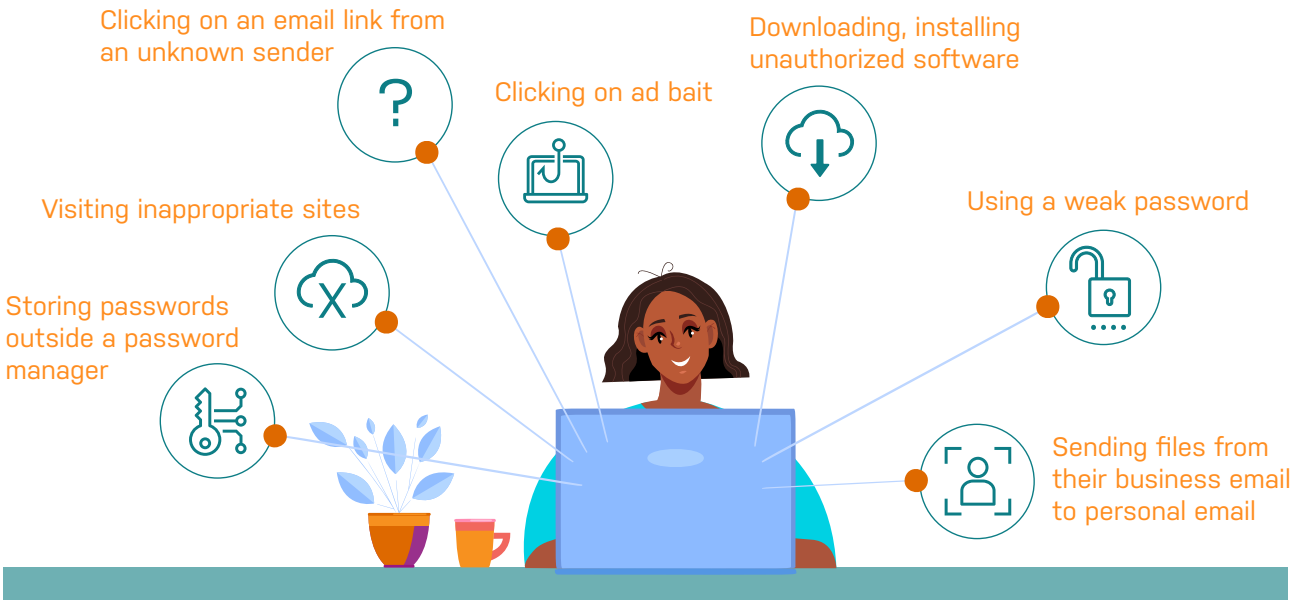
III. Deploy Adaptive Security and Tailor Employee Communications to Reduce Risk

I. Understand How Employee Security Decisions Impact Risk

Time and time again, **human error causes the biggest security vulnerabilities** in organizations. According to the 2020 Verizon Data Breach Investigations Report, human risk accounts for five of the top seven breach sources, including: password security, phishing, malware, data handling, and privilege abuse. These threats are not new to security leaders, however, forward looking CISOs are observing these threats with a completely different lens and recognize **reduction of this risk as an impactful source of business ROI**.

Daily decisions made by employees protect from or expose organizations to security incidents – and, unfortunately, more often than not, it's the latter. This risk permeates all aspects of the organization's security stack, from infrastructure, to identity and access, to the network and the cloud. Most breaches succeed as a direct result of employee errors, most often unintentional. Yet today's enterprises do not have adequate understanding into employee security decision making. As employees make thousands of security decisions everyday, **each wrong decision makes an organization more susceptible** to the next cyber attack.

While most organizations think of phishing emails as the only source of employee risk, the reality is much more worrisome. Here is a small example of the variety of security decisions employees make on a daily basis.



II. Identify Areas of Greatest Risk

Enterprise security and infrastructure solutions such as data loss prevention (DLP), end-point detection, malware, email scanning, identity and access management, cloud monitoring contain critical security incident data. Combining this with employee information from an HR system creates actionable insights around an employee's daily security decisions. This can highlight areas of greatest risk in the organization, a department, a location; allow you to better target remediations to drive better security outcomes and improve business performance.

Security teams can leverage this data and gain insights that help them answer critical questions to develop a better understanding of their security posture, such as:

- **Is my greatest risk from bad decisions when dealing with suspicious emails or is it with sensitive data disclosure?**
- **Are there patterns of risk in certain geographies?**
- **Which are your top performing departments?**
- **Which departments are your riskiest groups?**
- **Are our software investments having an impact on reducing our employees' risk?**

When security teams can answer these questions they are significantly better prepared to break away from a one-size-fits-all approach to security that impedes employee productivity.

For example, an employee with insignificant access privileges, who has a history of not clicking on phishing links and has a proven record of handling sensitive information safely does not need to be impeded by additional restrictions. On the other hand, a contractor who has access to financial data and has a history of downloading malware needs significant remediation to prevent future incidents from occurring. When enterprises have a better understanding of risk at the employee level they are well positioned to **achieve continuous compliance through adaptive security**.

III. Deploy Adaptive Security and Tailor Employee Communications to Reduce Risk

By monitoring and evaluating enterprise wide and individual employee risk you can take **informed and dynamic remediation on areas of risk that need it most**.

These insights also tell you which employees repeatedly make good security decisions. This can be used as a basis to allow more relaxed security controls such as a longer timeout between re-authentication attempts, relaxed Internet browsing policies, more time in between endpoint scans, etc. CISOs might even have the confidence to relax security controls with individuals who have a proven track record of resilience such as reducing how frequently they need to change their passwords or modifying policies.

When organizations have a deeper understanding of the risk type that employees present, **they can deploy security controls to reduce their greatest risk and enable business efficiency for employees who have proven better security decisions**.

Identified Level of Risk	Dynamic Remediation
Which are your top performing departments?	These individuals may not need further controls
Which departments are your riskiest groups?	The default setting for this group should be more strict and needs more attention
Are our programs having an impact on reducing our employees' risk?	Are controls working? Do additional remediations need to be taken that don't impede productivity
Who are your riskiest employees?	Is the risk high enough that privileged access should be logged, adjusted or revoked?

This approach is a fundamental shift in thinking. Traditionally, organizations think in the terms of zero trust and every component on the enterprise network needs to protect itself from each other.

> **Establishing and giving trust to an employee and/or an identity in an informed, distributed and dynamic manner contributes significant ROI to enterprise efficiency.**

The next critical step is often overlooked and helps remediate the root cause, human error. Security teams must foster a dialogue with employees and effectively communicate what they are doing well and where they are falling short to improve their security performance. CISOs who take this tailored and personalized approach to reducing risk have seen measurable reduction in risk as well as costly response clean up.

Elevate Security seamlessly integrates with existing solutions in the security stack to achieve this. To learn more about automating this approach talk to a member of the Elevate Security team today.

https://elevatesecurity.com/demo/

Security and Employee Data

Human Risk Insights

Elevate Security

About Elevate Security

Elevate Security, the leader in **Human Risk Management** software, helps enterprise security leaders measure, reduce, and communicate human risk to keep their companies safe from cyber threats. Elevate Security provides unique insights to CISOs by quantifying and analyzing human risk spanning the entire organization using security incident data. Armed with Elevate Security's insights, CISO's optimize security technology spend, focus monitoring and detection capabilities on high-risk groups, and strengthen their overall cyber defense strategy.

Elevate Security seamlessly integrates with existing solutions in the security stack to deliver more holistic insights. Medium and large enterprises across industries, from financial services, technology, healthcare and more, have increased cyber resilience by incorporating Elevate Security into their security infrastructure.

For more information, visit: https://elevatesecurity.com/