Elevate Security

Fall 2020 Edition

Global Employee Risk Insights Report

First-of-its Kind Analysis of Over 1.5 Million Employees' Security Decisions Across Industries

Introduction

Reassessing Your Risk-Based Approach in Today's Evolved Remote Environment

In order to reduce corporate risk, security leaders must identify and focus on the elements of cyber risk. (McKinsey & Company: The Risk-Based Approach to Cybersecurity: October 2019.)

Most enterprises have evolved beyond an emphasis on security foundational capabilities, such as the security operations center (SOC), strong authentication (MFA), etc. While this is important for organizations that need to build the security structure from the ground up, McKinsey & Company describes this 'maturity-based' approach as follows:

> **"It can never be more than a proxy for actually measuring, managing, and reducing enterprise risk.**
>
> **A more strategic, risk-based approach is imperative for effective and efficient risk management.**

CompTIA's State of Cybersecurity 2020 Report further validates this mindset, naming risk management as the number one organizational practice needed for a robust security posture.

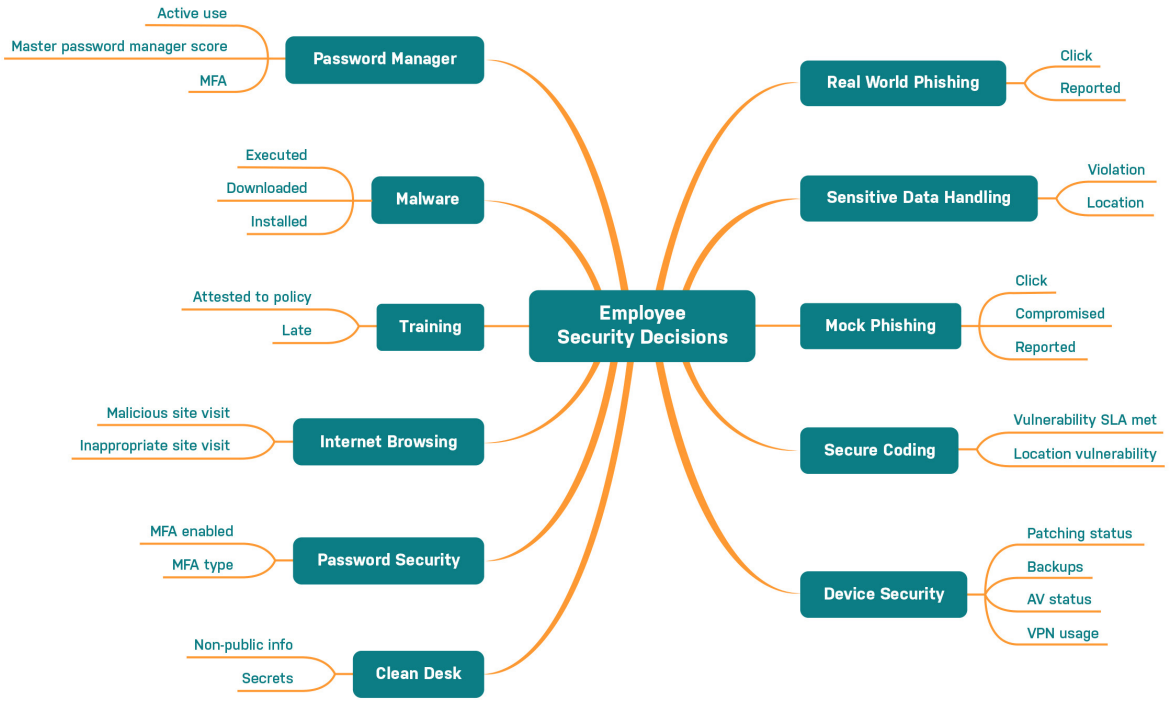
Simultaneously, the dramatic shift to remote work driven by the COVID-19 pandemic has also exacerbated new and existing risks, driving enterprises to reevaluate security practices. In fact, CompTIA's research reveals the increase in the remote workforce as the primary trigger for corporate security reassessment.

Understanding How An Employee's Security Decisions Impact Risk

As noted in the annual 2020 Verizon Data Breach Investigations Report, human risk has remained the top breach source for the past five years and currently accounts for FIVE of the top seven breach sources, including: phishing, password security, malware, data handling, and privilege abuse. Additionally, the CompTIA 2020 report writes that ***"employee error remains the primary component of most security breaches."***

Security decisions that employees make comprise the bulk of enterprise-wide vulnerabilities, making the reduction of this employee risk an impactful source of business ROI. This risk permeates all aspects of your organization's security stack, from your infrastructure, to identity and access, to the network and the cloud. Most breaches succeed as a direct result of employee errors, whether unintentional or intentional. Daily decisions made by your employees reduce or expose your business to security incidents – and, unfortunately, more often than not, it's the latter.

Yet today's enterprises do not have adequate visibility and understanding into employee security risk. As your employees make thousands of such decisions everyday, each wrong decision makes your 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.



Example of some of the decisions employees make every day that put your organization at risk

Integrating Actionable Employee Risk Insights into your Cyber Risk Framework

As companies move from a maturity-based to a risk-based approach for managing cyber risk, they must measure and monitor employee risks in the same way that they monitor other security vulnerabilities. Without that insight, it's impossible for the CISO to undertake a proactive risk-based approach to cover the entire spectrum of security.

To provide CISOs with greater visibility and actionable insights on employee aspects of cyber risks, Elevate Security has published the industry's first global research report on employee security decisions. This is a first-of-its-kind analysis of more than 1.5 million employee security decisions leveraging Elevate Security's unique and proprietary cross-company data set. With data-driven insights derived from millions of observed security actions aggregated from dozens of security tools onto the Elevate platform, these findings provide security leaders with unprecedented and real-world insights into employee security performance predictors.

By identifying which types of employees are most likely to fall victim to various breach vectors, security leaders can more effectively intervene to reduce such incidents. CISOs can:

- ✔ **Understand potential risks before incidents happen;**
- ✔ **Tailor preventative efforts more precisely;**
- ✔ **Apply data to improve internal policies;**
- ✔ **Adjust access and permission levels to groups and individuals and**
- ✔ **Engage executive support.**

In this inaugural edition of our groundbreaking research series, we uncover and assess the leading indicators of employee security incidents across the following four areas of employee risk:

I. Employees Who Are Most Susceptible to Phishing Attacks

II. Biggest Indicators for Password Manager Adoption

III. Correlation Between Training and Risky Security Decisions

IV. Why Security Training Falls Short in Reducing Risk

I. Who is Most Susceptible to Phishing Attacks?

Tenure—the Biggest Indicator

For this component, we measured employee responses to phishing emails. Did they click them? Did they enter their credentials into a compromised site? Did they report them?

Using the security actions data set, we analyzed which employees are most and least likely to succumb to phishing attacks. To break down the data into smaller and smaller subsets, we used decision trees – splitting the data based on the most predictive attributes. Our decision tree included splits on an employee's tenure in the company, whether they were a full-time or part-time employee, their location, and team size.

The data showed that tenure represents the strongest indicator of phishing resilience – higher than geography or an employee's position in the organizational hierarchy. **Those most likely to click on a phishing email are short-tenured contractors on large teams.** Whereas, the least likely to click are U.S. employees who have been with the company more than three years but less than 16.

Having a remediation plan in mind when such insights surface is always helpful. For each area of employee risk, we recommend a few things to consider when formulating the plan.

Steps for Remediation

- ✔ Require secondary defense such as strong authentication for employees who have been with your company less than three years or more than 16, as well as short-tenured contractors
- ✔ Focus your mock phishing campaigns on employees who have been with your company less than three years or more than 16

II. Biggest Indicators for Password Manager Adoption

Geography—the Biggest Indicator

To analyze password manager usage, we again turned to the decision data set. We found that, in the case of password manager adoption, geography was the highest indicator of employees most and least likely to use a password manager. In this scenario, tenure only showed a slight effect.

The results showed that U.S. employees who had been working for a company longer than 1.3 years were the most likely to use a password manager. On the flip side:

Employees in the Asia-Pacific region who had been working for a company longer than 1.3 years were least likely to embrace using password managers, reflecting the impact that geography can have on employee decisions.

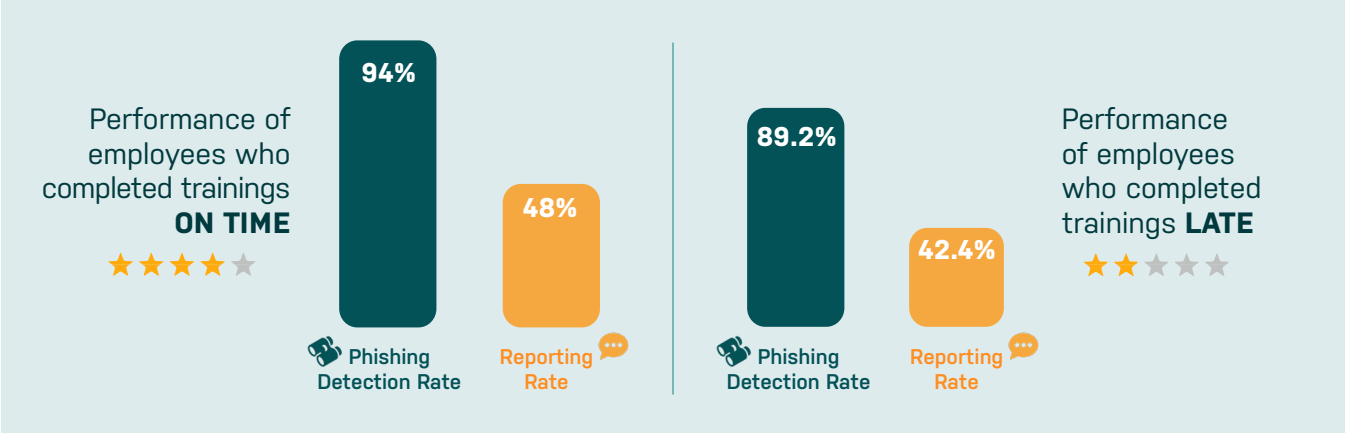
Steps for Remediation

- ✔ Create dedicated campaigns to encourage the use of password managers in Asia-Pacific countries
- ✔ Translate your communications and get input from local experts on cultural relevance to ensure the message gets delivered most effectively

III. Correlation Between Training and Risky Security Decisions

Can one easy-to-measure security decision predict another more critical one? In this scenario, we wanted to focus on something that almost all employees have to do within any organization today – take security training. We wanted to see if an employee's relationship to taking training on time could predict how they'll perform on phishing attacks.

We looked at data for employees who completed their security training on time versus those employees who completed their security training late. Across all of the companies and all of the employees we looked at, we found:



Employees who completed training late performed worse on both detection of phishing attacks and phishing reporting. While not a huge percentage difference (2% and 6%, respectively), it clearly shows that employees who are late on training perform worse. When you consider in connection with other HR attributes, such as geography or tenure, you find even more common groupings of people.

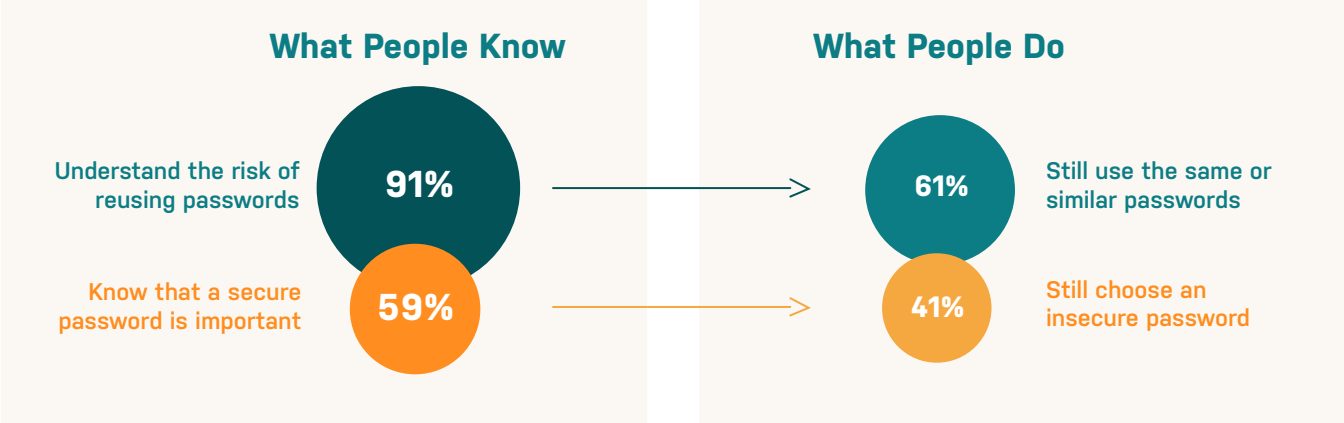
However, while the data shows that timely completion of training has an impact on security performance, it is still important to recognize overall training shortcomings. Most notably, research shows that an employee's security decisions do not necessarily correlate to an employee's knowledge of appropriate security protocols. This is explained further on the following page: **Why Security Training Falls Short in Reducing Risk**.

Steps for Remediation

- ✔ **Monitor employees who are regularly late on security training more closely for risky security decisions**

IV. Why Security Training Falls Short in Reducing Risk

Existing security training programs focus primarily on increasing an employee's knowledge about cyber threats and how to deter them. They do not monitor or measure whether the employee is actually making security decisions based on the knowledge gained through these training sessions. This approach results in a disconnect between desired outcomes and reality.



Data source: Ovum "Closing the Password Security Gap"

Conclusion

Take a Risk-Based Approach to Managing Employee Vulnerabilities

Increasing the effectiveness of your overall security strategy requires expanding your risk-based approach to quantify employee risk by monitoring employee's real-world security decisions and mitigating vulnerabilities caused by these decisions.

This groundbreaking research indicates, with statistical significance, that there are clear indicators that predict employee security performance. The indicators explained in this first-of-its-kind report can help security teams understand which employees are most likely to fall into breach categories, increase understanding of good and bad security performance, and adopt effective interventions to increase or decrease security controls based on employees' past security decisions.

Research Methodology

Employee data for this report was derived from Elevate Security's proprietary cross-industry and cross-company data set, covering security decisions made by thousands of employees worldwide. Company sizes ranged from one thousand to over forty thousand employees.

Over a period of 18 months, we observed employee security decisions, spotting key trends and unlocking actionable insights. Our analysis also encompassed human resource (HR) data attributes, including characteristics, such as: geography, type of position, i.e. full-time, part-time or contractor, tenure at company, team size and organization size.

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/