Elevate Security

Addressing Today's Biggest Cybersecurity Gap, 'Employee Risk'

When you know who is risky and why, you have a tractable problem that's solvable. Let's dig deeper!

Elevate Security helps organizations identify their riskiest people and automate safeguards to reduce workforce risk while continuously measuring progress. As part of this process, Elevate Security collects and analyzes data to identify actions and trends that drive successful customer outcomes.

Our recent findings? Wow, we think you'll be as impressed as our customers!

Findings for a Fortune 500 Enterprise

73%

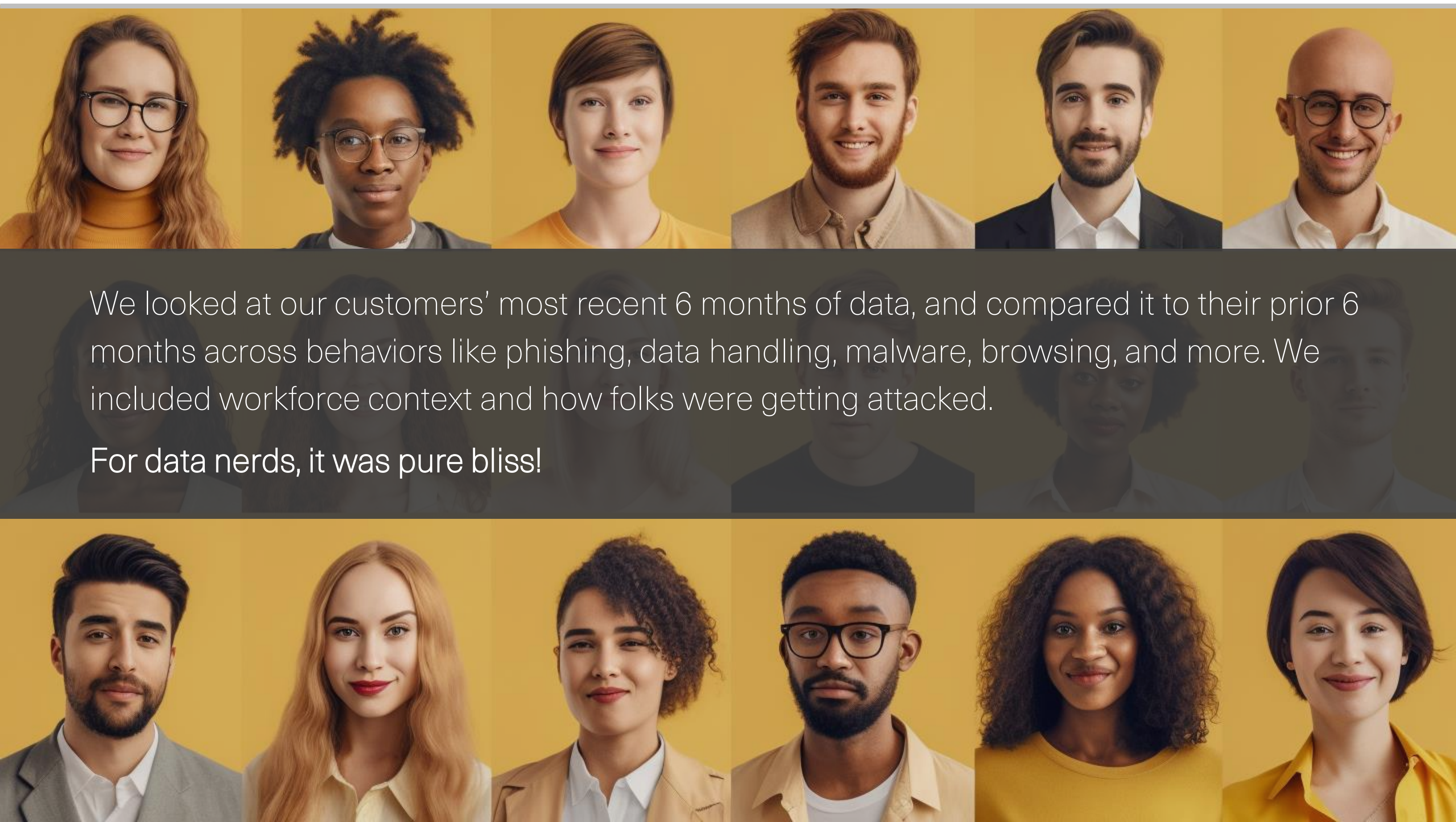
Reduction of **Sensitive Data Handling Incidents**

70%

Reduction of **Phishing Clicks (Real-World)**

373%

Increase of **Phishing Reporting**



We looked at our customers' most recent 6 months of data, and compared it to their prior 6 months across behaviors like phishing, data handling, malware, browsing, and more. We included workforce context and how folks were getting attacked.

For data nerds, it was pure bliss!

For a large **Financial Services** firm focused on reducing phishing risk, their use of Elevate delivered:

67%

Reduction in **Phishing Clicks (Real-World)**

210%

Increase in **Employee Phishing Reporting**

200%

Increase of **Phishing Emails Detected**

The ‘Ah Ha’ Moment

Our analysis kept finding similarly amazing outcomes, but a pattern became clear. Customers who only monitored workforce risk showed no statistically relevant changes in their average employee risk profiles month-over-month. This was huge, but why? Organizations deploying interventions and safeguards found massive improvements in reducing their workforce risk!

Use of Elevate interventions significantly reduces risk and your chance of incidents or breaches. Less obvious, they also reduce the amount of ‘whack-a-mole’ your security team has to do. And, our customers achieved these results while maintaining extremely high employee satisfaction scores.

Along our customers’ journeys, we’ve learned several key lessons

1 People are not one-size-fits-all and neither are solutions

Employees are unique. The CFO has a different risk profile than a junior engineer working from a remote office who started 5 days ago. Workforce context, role, access, behaviors, by whom and how they’re attacked, are all parts of the equation of understanding workforce risk and building cohorts.

Elevate analysis finds that 8% of employees are causing 80% of an organization’s security incidents. Applying a one-size-fits-all-approach to user security and training won’t solve for this dynamic. Imagine, if you were a car manufacturer and 8% of your parts were causing 80% of your reliability issues, you’d spend more time fixing the 8%. But, with employees we tend to ignore it. Elevate helps you change this dynamic by continuously identifying your high-risk hot spots and automating appropriate response.

2 You must intelligently (and automatically) manage employee risk

So much of our security telemetry is in disparate and disconnected systems, especially when it comes to people. As identity solutions become the new perimeter, we need to integrate these intelligence sources to stop employees becoming the primary attack vector, and slow the rise of social engineering and account compromise attacks.

This means building context and intelligence across our control technologies so we can automatically protect employees based on their risk profiles. Once you understand the risks, the protection options become clear.

- Employee X clicks on lots of phishing links? No worries, you can drive stronger email protection
- Employee Y is authenticating to a sensitive resource and has recent signs of account compromise activity? No problem, trigger a conditional access policy to require phishing resistant MFA, and restrict the user's access to critical resources

3 A gentle 'nudge' can go a long way :)

Employees generally want to do the right thing. Most "bad behavior" is unintentional, and sometimes a quick reminder can help course correct before bad habits build.

Periodic security training won't solve for that, but real-time, contextual 'nudges' based on behaviors absolutely will—as the findings above demonstrate!

- A new hire downloads software they shouldn't have? Easy. Let them know why that's a bad idea, right when they do it
- A contractor's nearing the end of their term and you're worried about them grabbing confidential IP before they leave? You're covered. Alert and remind them of policies as their last days approach

These small reminders (delivered over email, Slack, or MS Teams, etc.) drive big reductions in bad behavior. We find typically 20-30% across our customer base. That's 20-30% that your team doesn't have to go back in and clean up after!

Elevate Security

Identify and Safeguard Your Riskiest People

Insights from Robert Fly, Co-founder and CEO of Elevate Security

In my 20+ years as a practitioner building world-class security teams and organizations from scratch at Microsoft and Salesforce, I'd bought the best of email security, endpoint tools, gateways, identity systems, UEBA, and more. I tried 'best of breed' and 'best of suite'. But, my teams were still overwhelmed no matter how big the team or my budget was.

Rather than continue to hire more people and ask for more budget, we dug into the data we had, to try and understand where a dollar spent would have the biggest impact on reducing risk. Our findings:

1. About 90% of the issues we dealt with were 'run of the mill' problems — phishing, malware, data handling

2. Only about 8% of our employees were causing 80% of the issues we needed to clean up

...the takeaway? Most of the 'whack-a-mole' work had a human component to it. We'd largely ignored the people angle outside of some training content and phishing simulations. Most of our energy was spent on devices, networks, applications, and data. Not the people.

The technology we had purchased to protect our systems and people was failing. It was on us to do better, not to put the blame on employees.

This ultimately led to the start of Elevate Security, the first workforce risk platform for identifying and responding to high-risk people.

We welcome speaking with you about your workforce risk. Book a demo to learn more.

BOOK A DEMO