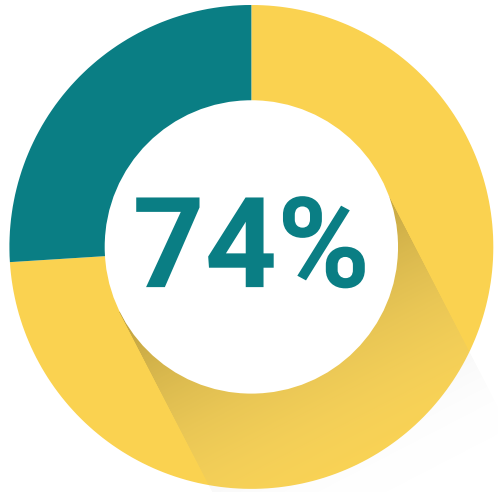
Elevate Security

Unintentional Insider Risk Mitigation:

The Essential Checklist to Bolstering Your Security Posture in 2024

Data is Everything

when just 8% of users cause 80% of security incidents.



of breaches involve the human element.
[2023 Verizon DBIR]

It's clear that if companies reduce their exposure to unintentional insider risk, it could have a major impact on their overall security posture.

Still, year after year, we hear the same stories of companies experiencing catastrophic losses due to a breach from the inside.

We have to move past the notion that broad, non-targeted security approaches are enough to protect our privileged information.

We have to act on data—but it's only useful if it gives us visibility into the individual risk of each user.

Digital Hygiene

Security Awareness & Training

Identity & Access Management

Incident Triage & Automation

It’s Time to Refresh

In 2024, every CISO should evaluate whether they’re acting on data to safeguard against insider risk in all of these areas.

By checking off the boxes in this checklist, you’ll ensure that you solve for the unique security vulnerabilities of each employee in your organization—rather than falling victim to arbitrary, one-size-fits-all security procedures.

Follow our checklist to strengthen your security posture against unintentional insider risk.

Digital Hygiene

While it may be the most basic solution to preventing a breach, digital hygiene is too often overlooked. Improving it at the individual level can have a significant impact on any company's cyber-readiness.

- **Implement a strong password policy.** Ensure that each employee is required to set a difficult password for every platform they have to login to.
- **Regularly refresh account credentials.** You should never go too long without requiring password resets for your employees.
- **Support employees with password managers and antivirus software.** Having these technologies in place doesn't just make it easier for employees to comply with your password policy—it relieves security burden.

- [ ] **Maintain individual user risk profiles.** You should be contextualizing the data pulled from your SIEM into insights that tell you more about the security posture of each employee.

- [ ] **Add risky employees to high watch lists.** Once you know the individual risk profile of each employee, you can start prioritizing the ones that need the most attention.

- [ ] **Assign behavior-specific training at an individual level.** Train employees based on their weaknesses. If they're most susceptible to phishing, assign training that focuses on phishing.

- [ ] **Notify employees when they've engaged in risky behavior.** With in-the-moment feedback, they're more likely to realize their mistakes and make adjustments for the future.

- [ ] **Incentivize employees to improve their security posture.** A positive security culture isn't built overnight. Motivate employees to be better stewards of your privileged information with incentives—and don't forget to commend them when they've made progress.

Security Awareness & Training

If just a small group of people are responsible for the vast majority of security incidents, then assigning everyone the same amount and type of training assignments isn't just ineffective—it's a waste of company time and resources.

Check these steps off your list to embrace a modern approach to security awareness & training.

Do it all with Elevate Engage

Elevate Engage ingests and analyzes data from across your enterprise to identify and score individual risk based on behaviors and attack history. With human risk score cards and real-time, personalized feedback, you can tailor your security and awareness training to each and every one of your employees.

Identity & Access Management

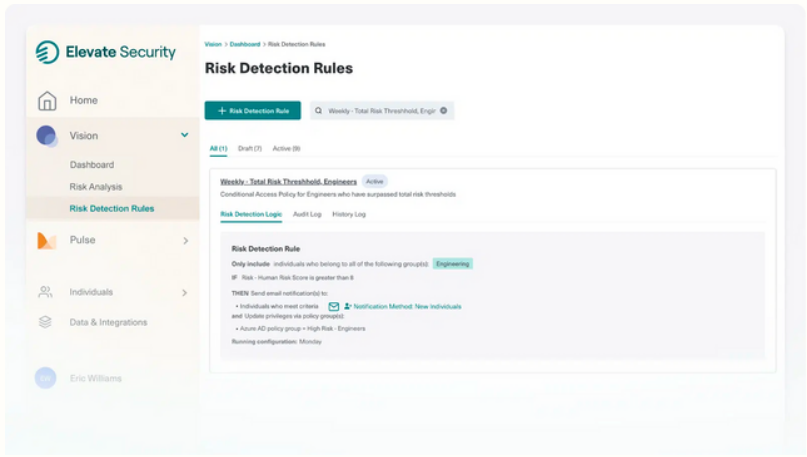
Even if your workforce is making great strides in their security habits, you should assume that someone, at some time, will fall for a social engineering attempt.

When that inevitably happens, you want to be sure that the threat actor is not able to access other systems in your network. Identity and access management can stop them in their tracks.

Do it all with Elevate Identity

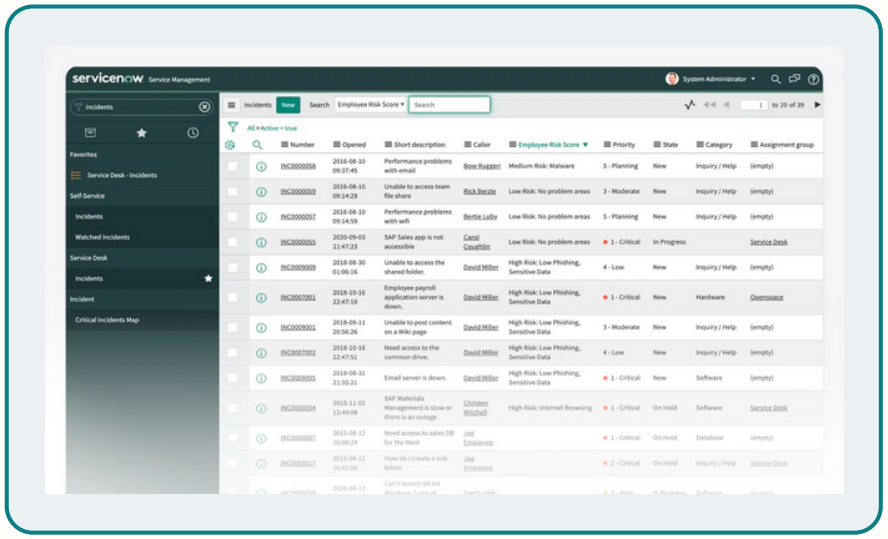
With Elevate Identity, verified threat signals provide context for all access decisions—allowing you to use risk intelligence as a control factor for approving, denying, or initiating conditional access requirements.

- ☐ **Set conditional access policies.** No employee should be given more access than their role or risk profile requires. Any given user should have to meet those requirements before they are given access to a system.
- ☐ **Require multi factor authentication (MFA).** This prevents threat actors from gaining access to a system if only one form of verification has been compromised. Requiring MFA at regular intervals of time within a system further strengthens its ability to stop threat actors.
- ☐ H**ave regular access governance reviews.** You should always be evaluating who in your enterprise needs access to what—especially after a security incident has occurred.



- **Integrate user risk data into case management workflows.** This empowers your help desk with the context to make data-informed decisions for service requests.

- **Set thresholds that automate risk responses.** Maybe a user is logging in from an impossible location or at an irregular time. You want to have triggers in place that can revoke access if any malicious activity is suspected—even when you're sleeping.



Incident Triage & Automation

The last step of any effective security program is to leverage automation so that your privileged information is protected around the clock and at scale.

Do it all with Elevate Control

Elevate Control injects user risk data into Security Operations tooling to accelerate and prioritize incident triage and response, enable better analyst decision making, and automate right sized control policies for your riskiest users.

Final Thoughts

A one-size-fits-all approach to cybersecurity can never stand against malicious actors who are tailoring their attacks to your employees' individual vulnerabilities. You need visibility into where those vulnerabilities exist. Only then can you take steps towards improving the overall security posture of your organization with tailored security measures of your own.

By moving through this checklist, you'll be able to shore up gaps in your security with right-sized, data-based strategies. Just remember that cybersecurity is an ongoing project. The constant refining of these strategies will safeguard your organization against an evolving threat landscape.

About Elevate Security

Elevate Security, founded in 2007 by two ex-Salesforce executives, focuses on providing organizations with the right technology and tools to mitigate insider risk. With a user risk profile, enterprises have more visibility into their cybersecurity than ever before by tracking user behaviors and evaluating them for risk. This way, employers have an inside look into their team's actions and can make adjustments to permissions and access as needed. In addition, the Elevate Security Platform enables your organization to take preventative action against cyberattacks, providing you with the data to do so. Please visit elevatesecurity.com for more information.