Commissioned by

Elevate Security

Elevating Human Attack Surface Management

A CYENTIA INSTITUTE STUDY IN COLLABORATION WITH ELEVATE SECURITY

Introduction

> HUMAN RISK PLAYED A ROLE IN 88% OF THE TOTAL LOSSES FROM THE LARGEST CYBER INCIDENTS OF THE LAST 5 YEARS.

In his 2008 essay, Bruce Schneier extols the virtues of the "Security Mindset". He argues that a particular type of thinking, one focusing not only on the functionality of a system but also on how it can be misused, is an essential way for security professionals to view the world.

If the "Security Mindset" was an important ideal back then, it is much more so today. Nearly everyone—not just security professionals—must be at least a little bit aware of the dangers they face when clicking through emails, selecting passwords, or installing new apps. However, the constant vigilance required by this mindset is simply asking too much of most people. And yet, we also can't just lock down everyone and everything around them without bringing the business to a grinding halt.

This challenge creates an impasse for organizations seeking to manage their human attack surface and raises some critical questions. What can be done to develop ongoing visibility into the full spectrum of risky employee decisions that undermine enterprise defenses? Is it possible to cultivate a "securer mindset" without paralyzing productivity for fear of cyber boogeymen in every URL? Finally, how do we mitigate the impact of the inevitable poor decisions employees make and provide them the right security protections based on their individual risk levels?

This report starts to answer these questions (and more) by mining through troves of sanitized data from Elevate Security. We unearthed tons of fascinating nuggets of knowledge from those mining operations, but we've decided to focus this report on some key lessons we learned about measuring and managing the human attack surface. Keen to know what those lessons are and how to apply them to your organization? Great, let's go!

Key Findings

Nearly two-thirds of major data breaches are tied directly back to human risk factors.

Human risk played a direct role in 88% of the total losses attributed to the largest cyber incidents of the last five years!

Security training and phishing simulation results in slightly lower click rates among users but has no significant effect at the organizational level.

Users with active password managers are 19 times less likely to download or execute malware than those without them.

Malware infections are 10 times more likely to occur among users at the bottom of the org chart than those at the top.

Human Attack Surface

The management of just about anything improves when we can measure it, and this is especially apropos when managing the human attack surface. However, before we can begin measuring the human attack surface, we need to know what it is. We define the human attack surface as "the sum total of people's actions, access, and security controls that impact an organization's risk". This attack surface is made up of individual employee risk - human risk - which is the probability and impact of any individual in a company making a good or poor security decision.

This definition certainly frames the wide scope of human attack surface and human risk, but we need more specificity if we hope to measure it. Thankfully, Elevate provides some helpful context: "*These decisions run the gamut from simply clicking on a phishing email to uploading sensitive data to the cloud or using weak passwords. As your employees make thousands of such decisions every day, each wrong decision makes your organization more susceptible to the next cyber attack. Each of these decisions is amplified or dampened by access levels these employees have and the controls we have in place to protect them.*"

We can infer from these examples that the human attack surface is a vital part of the overall attack surface that must be defended, and its risk is much broader than the classic insider threat archetype of rogue admins sabotaging systems or stealing information. Rogue admins and malicious actions by employees certainly warrant attention, but even the most upstanding and least privileged contractor does things daily that affect the risk exposure of the entire organization. As we'll show in the next section, it's these humdrum forms of human risk that prove to be the most insidious.

How do employee actions lead to risk?

To help demonstrate the multifaceted dimensions of the human attack surface, we'll leverage Verizon's long-running and well-respected Data Breach Investigations Report (DBIR). The 2020 DBIR analyzed nearly 4,000 breaches from 81 different contributors spanning law enforcement and other government agencies, security vendors, service providers, and incident response teams from around the world.

Our goal here isn't to provide a comprehensive treatise on the risk ramifications of human decisions and actions. Consistent with this goal, we present a sampling of statistics from the DBIR in a consolidated format on the following page to quickly set the stage for our own analysis. The DBIR serves as a lens through which we can view and measure how human risk manifests itself in security incidents. Understanding your human attack surface can be extremely helpful to your defense strategy. And as is clear, the "human element" in security breaches is as pervasive and diverse as humans themselves.

> **"ALL TOLD, OBSERVABLE FORMS OF HUMAN RISK PLAYED A DIRECT ROLE IN 61% OF EXTREME LOSS EVENTS INCLUDED IN THE IRIS XTREME. EVEN MORE DAUNTING IS THAT THESE HUMAN RISK FACTORS RACKED UP A PRICE TAG OF $15 BILLION — THAT'S 88% OF THE TOTAL LOSSES ATTRIBUTED TO THE LARGEST CYBER INCIDENTS OF THE LAST FIVE YEARS.**

Of all data breaches examined in the 2020 Verizon DBIR:

- **30%** of breaches involve internal threat actors
- **8%** of breaches involve misuse actions
- **20%** of breaches involve error actions
- **22%** phishing and other social engineering tactics
- **29%** of breaches target humans as a compromised asset
- **40%** of malware breaches employ password dumpers
- **37%** of malware breaches prompted users to click email links
- **13%** of malware breaches prompted users to execute attachments
- **80%** of hacking involves brute force or the use of lost or stolen credentials

How risky is human risk?

The big pile of somewhat disparate statistics from the DBIR in the box above might have you wondering "*Okay, but how big a deal is human risk overall*?" It's a good question, and we definitely don't want anyone to lose sight of the forest for the trees. So, let's briefly size up the human risk forest.

Most sources generally agree that risk involves the frequency and impact of adverse events. We'll tackle the frequency part of the risk equation first, and to do that, we'll once again return to the DBIR. Because incidents can involve multiple aspects of human risk referenced above (i.e., insider misuse and social engineering), we can't simply sum up all the percentages to derive the overall frequency. Thankfully, the people behind the DBIR are awesome and were willing to do the necessary calculations for us.

The result is eye-opening to say the least. Nearly two-thirds of the 3,950 breaches analyzed in the 2020 DBIR tie back *directly* to human risk. And that number gets even bigger if you include contributing factors upstream of the breach such as insecure software development and poor patch management. Suffice to say, human risk plays a role in most security incidents.

But what about the impact of these events? The DBIR doesn't focus on losses, so we'll turn to another source for measuring this side of human risk. The Cyentia Institute's Information Risk Insights Study (IRIS) 20/20 "Xtreme Edition" analyzes ~100 of the largest cyber loss events of the last 5 years. Similar to our process with the DBIR, we selected various elements of human risk evident in that study.

Overall, observable forms of human risk played a direct role in 63 of the 103 (61%) extreme loss events included in the IRIS Xtreme. Even more daunting is the fact that these human risk factors racked up a price tag of $15 billion—that's 88% of the total losses attributed to the largest cyber incidents of the last five years! The enormity of the human element in cyber risk is clearly something organizations cannot afford to ignore.

Indicators of Human Risk

MATERIALS AND METHODS

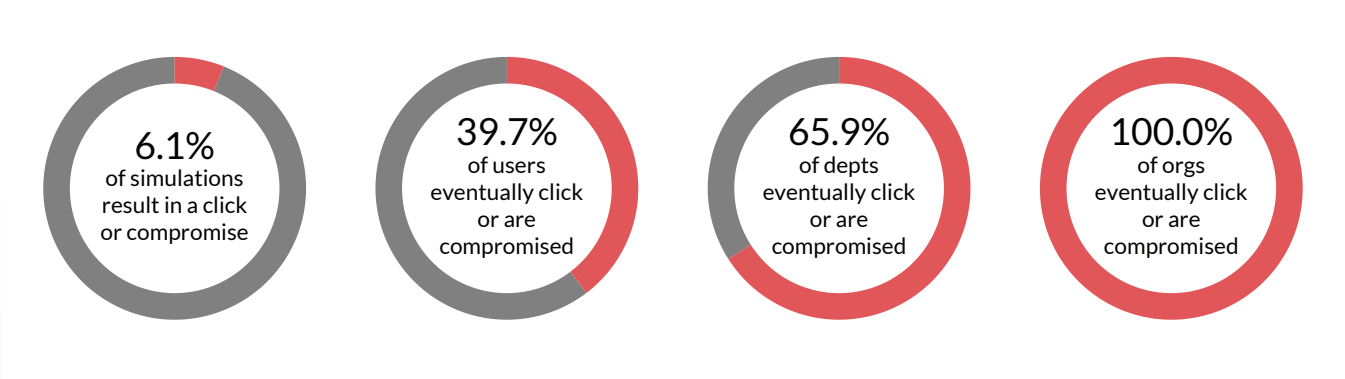
The analysis in this report was, unless otherwise cited, conducted on data provided to the Cyentia Institute by Elevate Security. The data includes 4.5m unique user actions taken by 114k users spread across more than 2,000 organizational departments and aggregated in elevate security's data platform. The data is from early 2018 to 2020. Not all users or departments measure all types of risk, so each result is reported on the subset of complete data. All stated relationships are statistically significant at the $p < 0.05$ level. Any regression results on continuous data (e.g. Figures 5 and 7) were obtained using beta regression to ensure that assumptions on the bounds of the dependent variable (e.g. "percent clicked") were satisfied. For any differences in proportions (e.g. Figure 7) a binomial proportion confidence interval was calculated using the Wilson method and was used to conduct a statistical test.

Now that we know what human risk is and what it looks like, let's explore some ways in which it might be visible or measurable within an organization. For this, we turn from the published statistics of the DBIR and IRIS Xtreme to the data collected within the Elevate Security Platform.

The last section established the broad scope of human risk factors in major incidents, so it's evident that the behaviors used to evaluate it must exhibit equal breadth. In keeping with this principle, we sampled various risk-relevant data points from the Elevate Platform. Think of these as some of the everyday outworkings of human risk that, ideally, can be monitored to help manage organizational exposure.

Since phishing is top of mind for human risk and is one of the earliest detectable actions in the chain of events leading to security incidents, let's start there. Have you ever wondered why cyber threat actors, from bottom-rung criminals to upper-tier national military units, incorporate phishing into their tactics, techniques, and procedures (TTPs)? Figure 1 illustrates the answer more clearly than even the savviest cyber threat intelligence analyst ever could: because it works.

Figure 1: It's inevitable that someone in the organization will click on phishing emails.

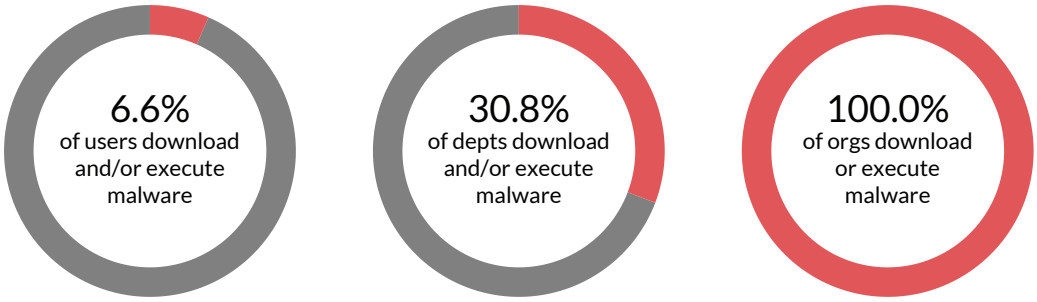


Many organizations understand the pervasiveness of phishing and thus run simulated exercises to raise awareness and strengthen resistance. In isolation, these phishing simulations offer some encouragement; only 6% result in users getting hooked. However, across multiple simulations, the encouraging signs begin to wane as almost 40% of users fall for the phish. If we continue rolling results up the organizational hierarchy, two-thirds of departments get duped. And when we evaluate click rates across the entire organization, we see that it is certain someone eventually will take the bait.

We see a similar progression when it comes to malware infections. Over the course of a little over a year (13.5 months), a small percentage of users (~7%) execute or download malware but this number grows to 31% across departments. And once again, the chances of someone introducing malware to enterprise assets balloon to 100% at the organizational level.

Oftentimes, phishing and malware steal user credentials that threat actors will leverage to gain deeper access into the environment and/or use in additional attacks. Exploiting default or weak passwords is another popular tactic as is apparent from the breach stats shared earlier in this report. It's logical, then, that using tools like multi-factor authentication (MFA) and password managers are important steps towards mitigating human risk.

Figure 2: It's inevitable that someone in the organization will download or execute malware.



Unfortunately, not everyone takes advantage of such tools. Less than one-third of users in the organizations we sampled had password managers installed and even fewer (25%) used them actively. The population of users with MFA enabled for their password manager dropped lower still (7%). This may not seem like a big deal, but we'll soon see that practices like this correlate more strongly with human risk than you might think.

Figure 3: Adoption of password managers by end users remains (too) low.

Among these various indicators of human risk, we see one overarching—and very critical—message: human risk might not be apparent at the individual level but becomes ubiquitous at the organizational level. Effective human risk management isn't just a matter of changing people's behavior. It requires a more proactive approach to mitigating risk by identifying which parts of the organization are susceptible. How targeted are these individuals and what level/scope of access do they have? What security controls should be put in place to mitigate risk? How can organizational risk culture be steered as a whole?

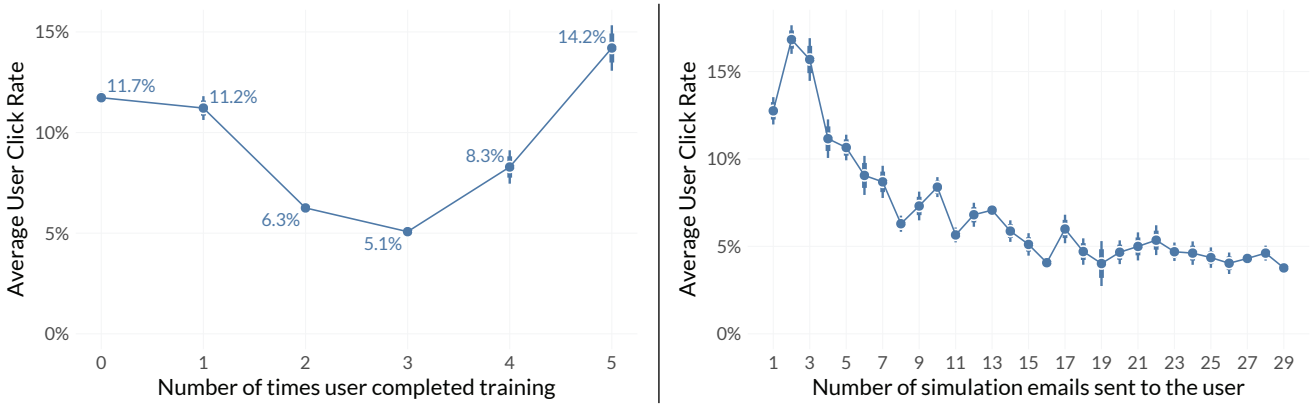
Lessons in Managing Human Risk

The previous section shows that it's possible to see indications of employee actions that amplify human risk without having to suffer a major incident or loss. We now seek to understand how human risk factors relate and how organizations can intervene and/or influence less risky behavior. In keeping with the exploratory nature of this goal, we present this section as a series of vignettes that share insightful lessons for managing human risk.

1: Training doesn't solve Human Risk

Security awareness training and phishing simulations are often the first lines of defense drawn around human risk. It's certainly an understandable approach given the breach statistics observed earlier. But questions about the actual effectiveness of training and simulation programs abound. We can teach users not to click but do those lessons stick?

Figure 4: Training and simulation help to a certain extent, but won't drive click rates to zero.



To that question, Figure 4 offers a reason to take hope as well as take heed. The left chart in Figure 4 shows that phishing click rates among users with three rounds of training (5%) drop to less than half that of untrained employees (12%).[1] So far, so good. But as simulations and training pile up, we never get to a zero click rate (or even close really). Too much of a good thing can be counterproductive and that appears to be the case here. Users with five training sessions are actually more likely to click than those with little to no training!

We don't see such a dramatic reversal in effectiveness for phishing simulations, but there's definitely evidence of diminishing returns from chumming inboxes with fake phish. Click rates drop pretty quickly from ~15% following the first few simulation runs but never seem to push below the 5% threshold. Effective programs need to find the right balance between user discernment and desensitization because over-training and over-simulation are valid concerns. So, while training and simulation might help some users, they won't solve the human risk. That means we need to find other ways to address it.

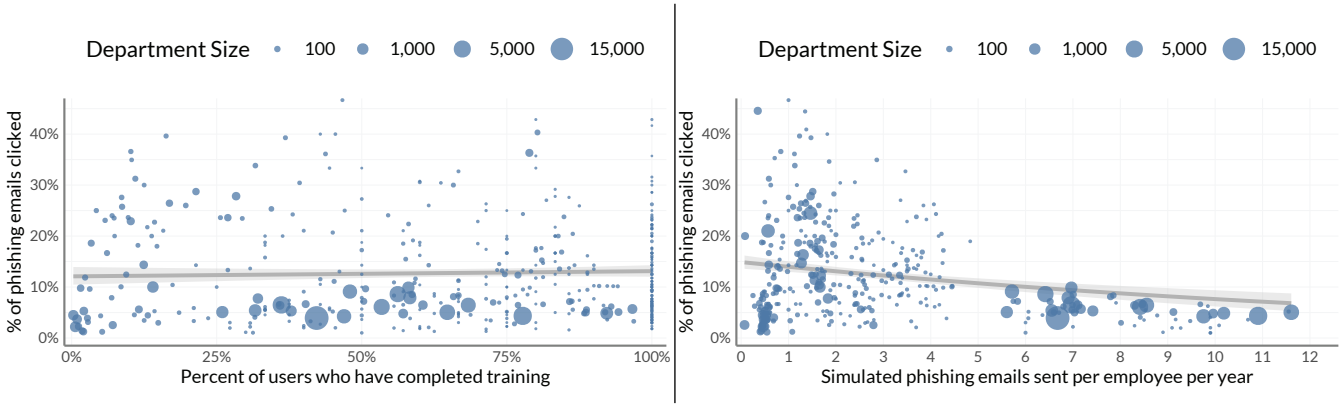
1 Note that we make no distinction about the format, content, or quality of training here. We did not have that information available.

2: Groups are even harder to manage than people

Training and simulation can have a limited effect on the risky behaviors of individual users, but do we see meaningful change in risk exposure at the organization level? The data gives mixed (and not extremely encouraging) signals on this topic.

Think of Figure 4 as an organizational version of Figure 5. Each dot represents a department and the position along the vertical axis indicates the percentage of users in each department that clicked on a phishing email. The chart on the left shows the effect of training pervasiveness on click rates. As you might infer from the flat regression line and the random scattering of dots across the plot, the effect is not significant. In other words, pushing for 100% security training compliance won't solve your firm's phishing problem (by itself).

Figure 5: At the departmental level, increasing training and simulation has little to no effect.



The chart on the right of Figure 5 shows something similar, except we're now testing the frequency of simulated phishing attempts. Here, the dampening effect on departmental click rates is significant. Departments with fewer than five runs per employee are all over the place, while those with higher numbers show less variation. This could be a sign of maturity and/or the positive benefits of long-term organizational commitment to combatting phishing.

> **EFFECTIVE PROGRAMS NEED TO FIND THE RIGHT BALANCE BETWEEN USER DISCERNMENT AND DESENSITIZATION BECAUSE OVER-TRAINING AND OVER-SIMULATION ARE VALID CONCERNS. SO, WHILE TRAINING AND SIMULATION MIGHT HELP SOME USERS, IT WON'T SOLVE THE HUMAN RISK. THAT MEANS WE NEED OTHER WAYS TO ADDRESS IT.**

SPOTLIGHT: THE CYBER CIRCADIAN RHYTHM

While not a panacea, the previous sections suggest that simulated phishing trials are a promising component in a human risk management program. When designing those simulations, it would seem reasonable to assume that they should mimic real-world phishing to the extent possible. We were curious to observe, therefore, that those trials march to a very different drum than real phishing attacks.

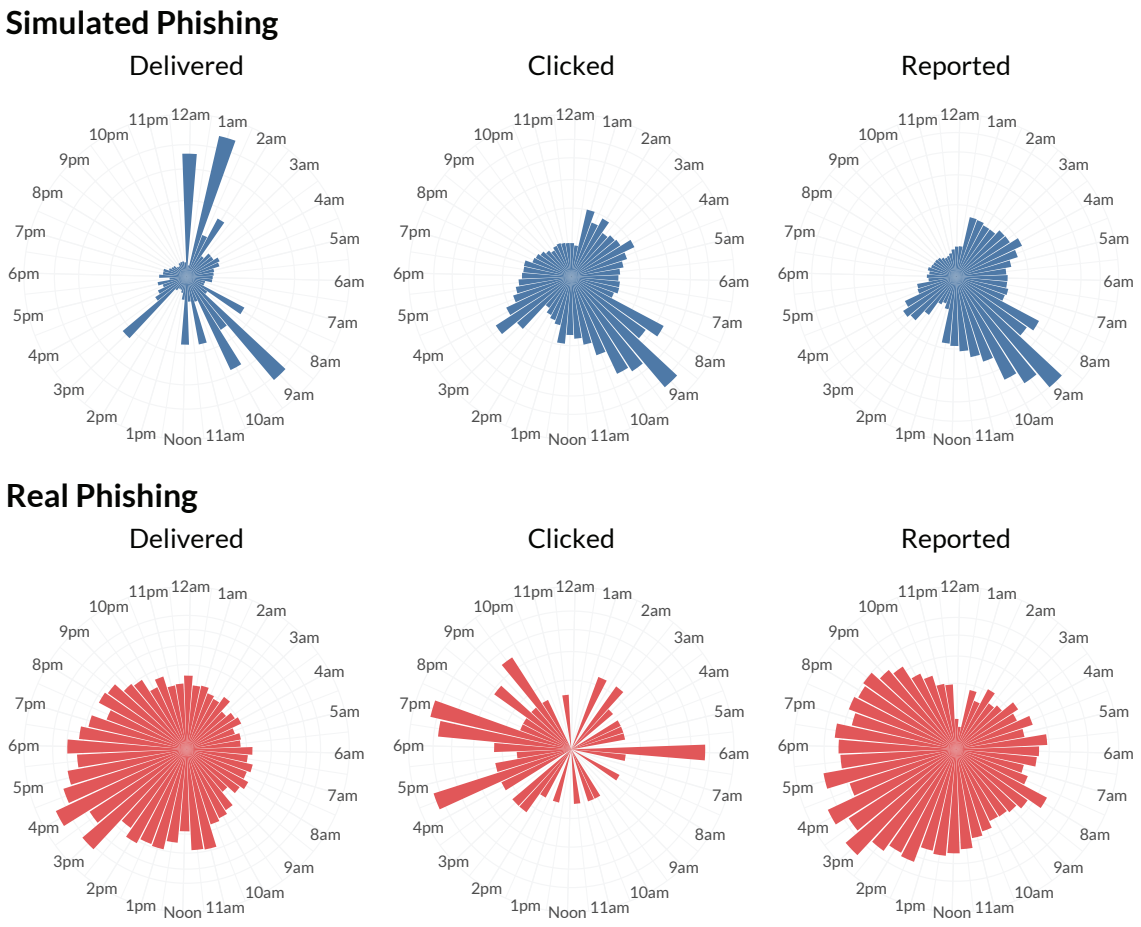


Figure 6: The timing of simulated and real phishing activities doesn't align.

As per Figure 6, real phishing emails are sent around the clock with a noticeable uptick around quitting time. Simulations have a far more artificial, scheduled rhythm. The timing of user interaction differs as well. Phony phish are most likely to be clicked or reported in the morning, but interactions with real phish align more closely with when they were sent.

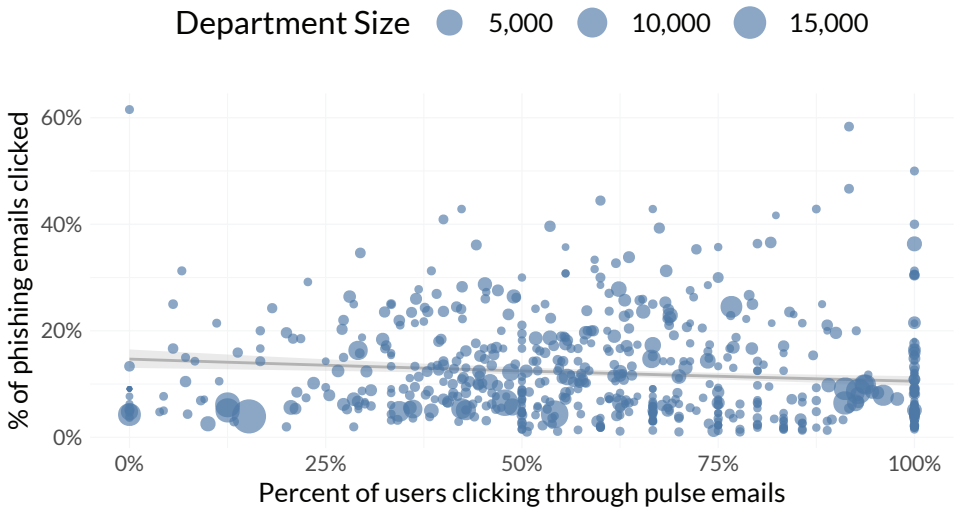
Why does this matter? Well, we can't help but wonder how this affects the reliability of results from phishing simulations. If the sports tenet of "practice like you want to play" has any application here, we'd want to see as little disparity as possible between real and simulated phishing events. And if the timing of that is off, we can't help but wonder what else might be off too.

3: Benchmarking is better than a briefing

Training and phishing trials aren't the only ways to foster more secure behaviors among your employees. Perhaps a carrot could do more than yet another training schtick. The "Pulse" scorecards sent to Elevate customers offered a way to test this theory. Pulses are personalized emails sent to users that contain key insights on their security performance and tools to help them improve that performance.

The format of Figure 7 should be familiar by now as should the basic result. A high engagement rate with Pulse emails won't ensure your department will win the security award, but on the other hand, this simple benchmarking tool is more effective than shoving users through another training course. More broadly, this hints that strategies like benchmarking and proactive actions may hold greater promise for reducing human risk than mandatory or punitive interventions.

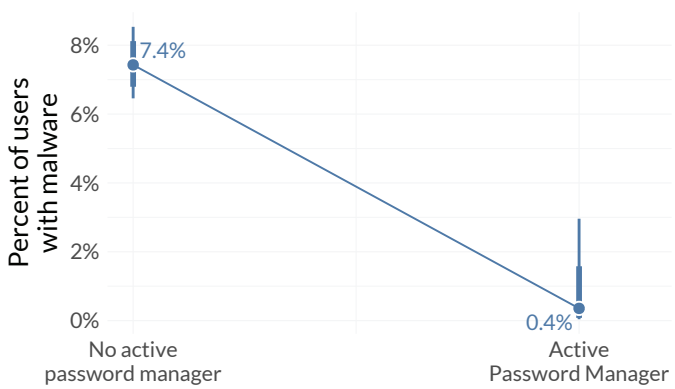
Figure 7: Regular updates that benchmarks human risk performance have more effect than training at the department level.



> **MORE BROADLY, THIS HINTS THAT STRATEGIES LIKE BENCHMARKING AND PROACTIVE ACTIONS MAY HOLD GREATER PROMISE FOR REDUCING HUMAN RISK THAN MANDATORY OR PUNITIVE INTERVENTIONS.**

4: Equip users to do the right thing

The last vignettes demonstrate that slides and simulations have at most a very limited effect on changing risky behavior. But risky behavior is more than just emails and training, so let's explore a bit. Based on the fact that exploiting weak passwords is a favored technique of Internet miscreants, Elevate encourages organizations to use password managers. But does equipping users with these tools correlate with reduced levels of human risk? You betcha!



As per Figure 8, users with active password managers are much less likely to download or execute malware. Why is that? It's hard to know for certain without additional tests, but it seems reasonable to infer that good security behaviors in one area roll over to good behaviors elsewhere. This also suggests that equipping users with useful tools may help them in following corporate security policies and procedures.

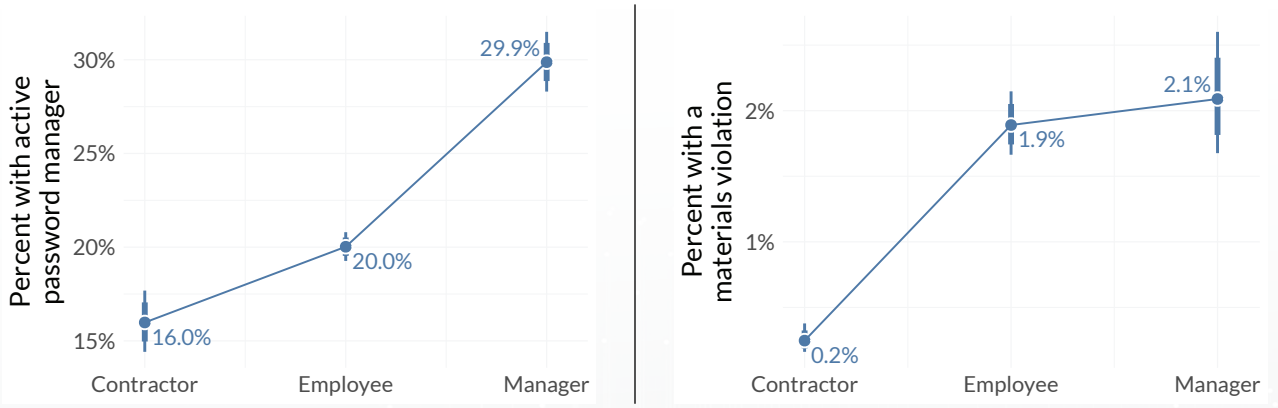
Figure 8: Using a password manager correlates with positive security outcomes like less malware.

5: Human risk is a role-playing game

Speaking of following the rules, who do you think exhibits the best security behavior—managers, employees, or contractors? If you suspect that might be a trick question, you'd be correct. The answer depends on which behaviors you deem most risky.

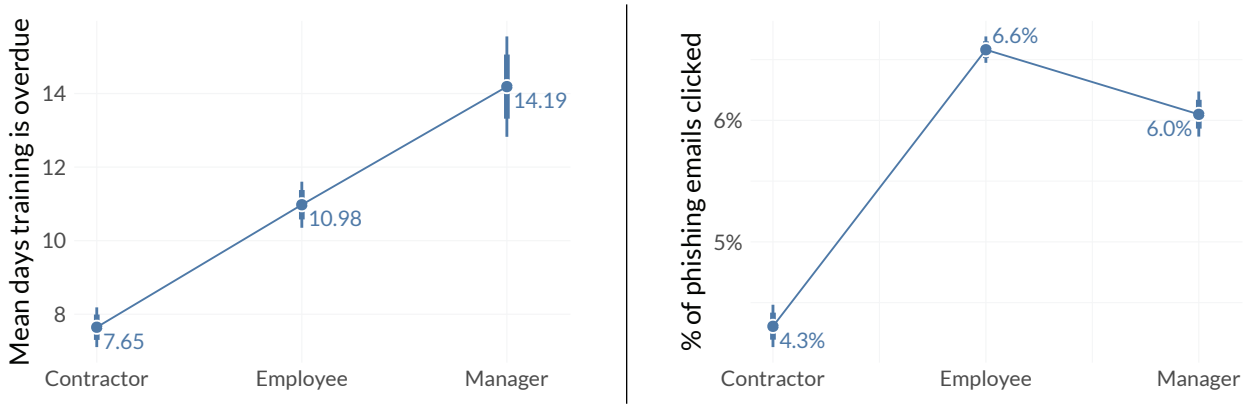
Figure 9a (below) and 9b (following page) compare these different organizational roles across four behavioral dimensions. Scanning them, we see that managers get a gold star for password manager adoption, but a frowny face for clean desk materials violations and missing training deadlines.

Figure 9a: The challenges of human risk differ among different types of employees.



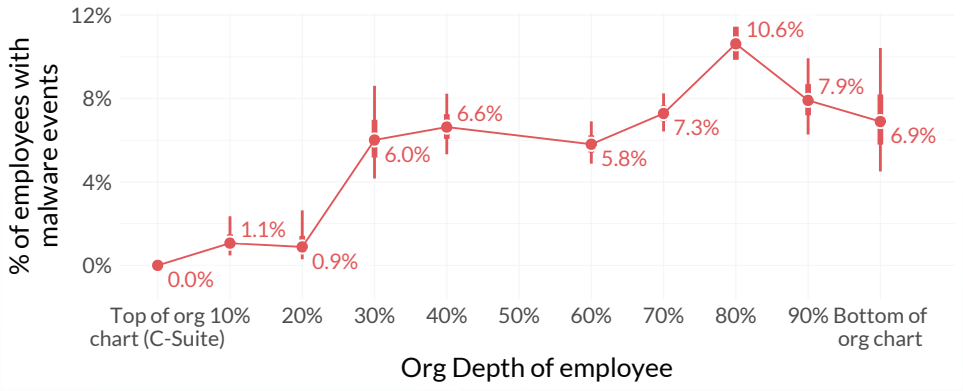
Rank and file employees generally fall between managers and contractors but win the Most Likely to Become Phish Bait award at the annual corporate shindig. Contractors have a pretty good track record of comparably low click rates and clean desk violations, but that accomplishment should be weighed against the fact that they receive fewer emails and don't often have permanent desks. As a reminder that human risk factors are always evolving, things like clean desk violations become less of an issue as more and more people work from home.

Figure 9b: The challenges of human risk differ among different types of employees.



We can't include all these charts in the space remaining, but we also observed that factors like the shape and depth of the organizational hierarchy influence behavior. For example, wide departments are less prone to phishing, while taller have fewer malware incidents. Malware is also more common toward the bottom of the org chart (see Figure 10). We're not saying you should restructure your entire organization; the main point here is that demographics seem as important to assessing human risk as the interventions designed to reduce it.

Figure 10 Employees lower in the org chart are more likely to have malware infections.



> **"THE MAIN POINT HERE IS THAT DEMOGRAPHICS SEEM AS IMPORTANT TO ASSESSING HUMAN RISK AS THE INTERVENTIONS DESIGNED TO REDUCE IT.**

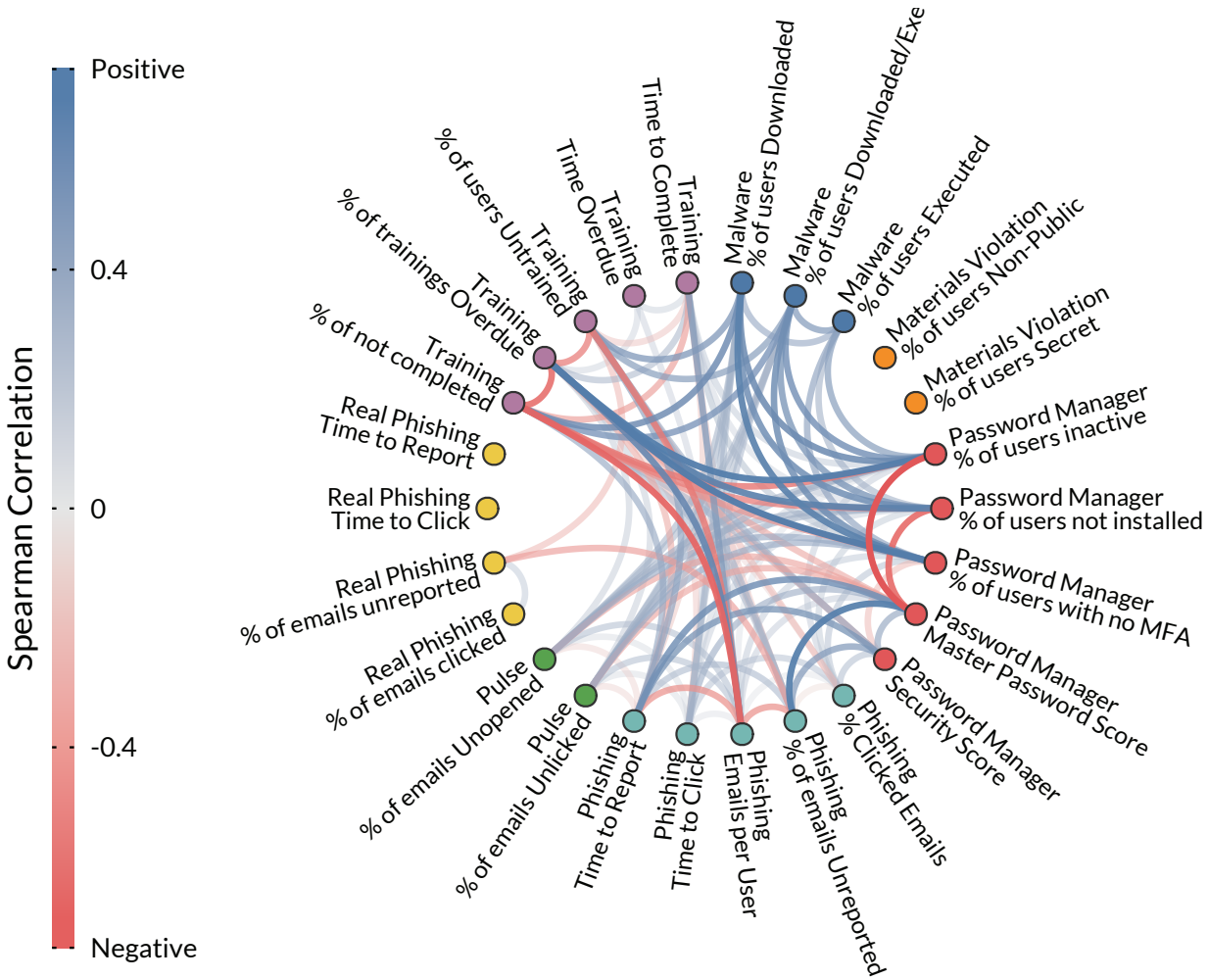
In Conclusion: We're Just Getting Started!

We enjoy the research we do, particularly when it involves great partners like Elevate Security and interesting topics like human attack surface management. And when that's the case, it's often hard to draw things to a close and say goodbye. So, instead of saying goodbye, we'll open the door for future research excursions into human risk.

From the vignettes in the previous section, it's clear that human risk factors are very complex and interconnected. We kept ourselves to bivariate analysis (does x correlate with y?), but the data yearns for more advanced multivariate analysis. The more we poked around, the more we realized that human risk is a tangled web that doesn't always work like we think it should. In the future, we hope to show more analysis of all the ways Elevate measures both organizational and human risk.

Speaking of a tangled web—check out Figure 11. It's our denouement of bivariate analysis. You'll find many of the risk factors discussed in this document along with others we never mentioned. The boldness of the lines connecting those factors indicates how strongly they correlate and the color marks the direction of that relationship (positive or negative).

Figure 11: The relationship among human risk factors is dauntingly complex but cannot be ignored



That's a lot to introduce in a conclusion, especially since we're not planning to unravel it with commentary. We're just setting up future research here, remember? For us, the relationships among risk factors in Figure 10 reveal dozens of threads we want to pull to see where they lead. Though we can't pull them right now, we do hope you'll join us in pondering over them until we can follow the threads of human risk in future research. But don't get tangled up!

OK...But what can I do now?

It's understandable that "we're gonna do more research" probably isn't the solution you were hoping for at the end of this report. But it is the solution that the problem demands, and as researchers, we have to be honest about that. However, that doesn't mean you can't start doing things right now that will improve human risk management for your organization.

Serious consideration must be given to understanding the Human Attack Surface within your enterprise. Human Risk as a critical part of that attack surface can and should be measured as part of a comprehensive cybersecurity framework. Benchmarked visibility into human risk along with targeted actions that can help protect the organization from risky employees can go a long way in creating the foundation for a robust cyberdefense strategy. In particular:

1. As a starting point, benchmark your organization's level of human risk relative to peer organizations and gain visibility into your human attack surface.
2. Adopt dynamic and adaptive security controls based on individual end user security assessments rather than one-size-fits-all controls.
3. Don't rely on security awareness training or more phishing simulations to address human risk because it's more than just a knowledge problem.