

mimecast

High Risk Users and Where to Find Them

A CYENTIA INSTITUTE STUDY BASED ON DATA FROM ELEVATE SECURITY (ACQUIRED BY MIMECAST)





EXECUTIVE SUMMARY

It's a horror story that many organizations are familiar with—an employee clicks a link or visits a website, and chaos ensues. At best, it's just a minor disruption. At worst, business continuity is broken, and an organization's critical infrastructure is at risk. Regardless of the outcome, managing human risk is a major part of business today. In this report, we dive into what makes workers high risk, where those high risk users spend their time, what are their riskiest behaviors, and what that might mean for your organization's security.

Key Findings



High risk users are the top quartile (75th percentile or above) of users in an organization who have had at least one instance of risky behavior, or event.



There aren't very many of them, but their impact is felt across the organization.



High risk users are responsible for:

- 41% Of all simulated phishing clicks
- 30% Of all real-world phishing clicks
- 54% Of all secure-browsing incidents
- 42% Of all malware events

High risk users are everywhere in the organization chart, but some departments have more high risk users than others.



Customer relations departments have a higher percentage of high risk users when compared to it departments.



In turn, IT departments have a higher percentage of high risk users when compared to product departments.



Clicks on simulated phishing are the most common high risk behavior. However, there isn't a correlation between high risk users who click on simulated phishing links and high risk users who click on real world phishing links.

“

At every part of the process, knowingly or not, people can make decisions that negatively impact their organization.

For decades, enterprise information security programs have tried to mitigate “human risk” by implementing various types of training and checkpoints.

But do these types of processes actually work?

Introduction

You’ll be hard-pressed to find a security professional that hasn’t heard the cliché, “people are the weakest link in the chain.” And there is a good reason for that. In the process of doing their daily work, knowingly or not, people can make decisions that negatively impact their organization. For decades, enterprise information security programs have tried to mitigate “human risk” by implementing various types of training and checkpoints. But do these types of processes actually work?

According to the 2022 Verizon Data Breach Investigations Report (DBIR), 82% of all data breaches involve human interaction. This report might lead us to believe that all human interactions are inherently dangerous. However, the findings in our last report offer some solace—most users are not risky, but a tiny percentage carry a high risk. We previously found that 76% of users have never clicked a phishing link in an email in contrast to the 4% of users that are responsible for 80% of phishing incidents. Along those same lines, while 93% of users have never had a malware incident, 3% are responsible for 92% of all malware events.

So, while most users aren’t inherently risky, a tiny percentage of users can be considered “high risk.” For this report, the Cyentia Institute analyzed almost eight years’ worth of data from Elevate Security (acquired by Mimecast)—from June 2014–July 2022. Using what we have learned about users from the previous report, we’ll be taking a deeper look into what a high risk user is, where they work in your organization, and how they impact organizations like yours.

What is a High Risk User?

“The call is coming from inside the house”

Let’s kick off by defining what makes a user high risk. Using what we know from our past analysis, a high risk user has a history of engaging in risky behavior at a higher rate. The vast majority of an organization’s users do not fall under this definition, but a small yet impactful group of users do.

Risky Behavior

Now let's make the definition of high risk more concrete. What exactly is "risky behavior" and how much does a user have to do to be high risk? We define risky behavior, or high risk behavior, in three different categories: Phishing, Malware, and Browsing.

Phishing - Real and Simulated

For our purposes, we will discuss two forms of phishing - simulated and real. In our data set, we logged over 3.4 million simulated phishing emails sent. The overall click rate? 7.6%. On the other hand, malicious actors commit real phishing attacks and they're the real deal. When a high risk user clicks on a real phishing link, the impact can be disastrous. In our data set, we logged over 1.8 million real phishing emails delivered, with an overall clickthrough rate of 4.1%.

There is a pretty intriguing difference right off the bat. We have almost three times as many simulated phishing emails sent as real phishing emails. This difference could signal that organizations are zealous about minimizing the number of high risk users by implementing more awareness training.

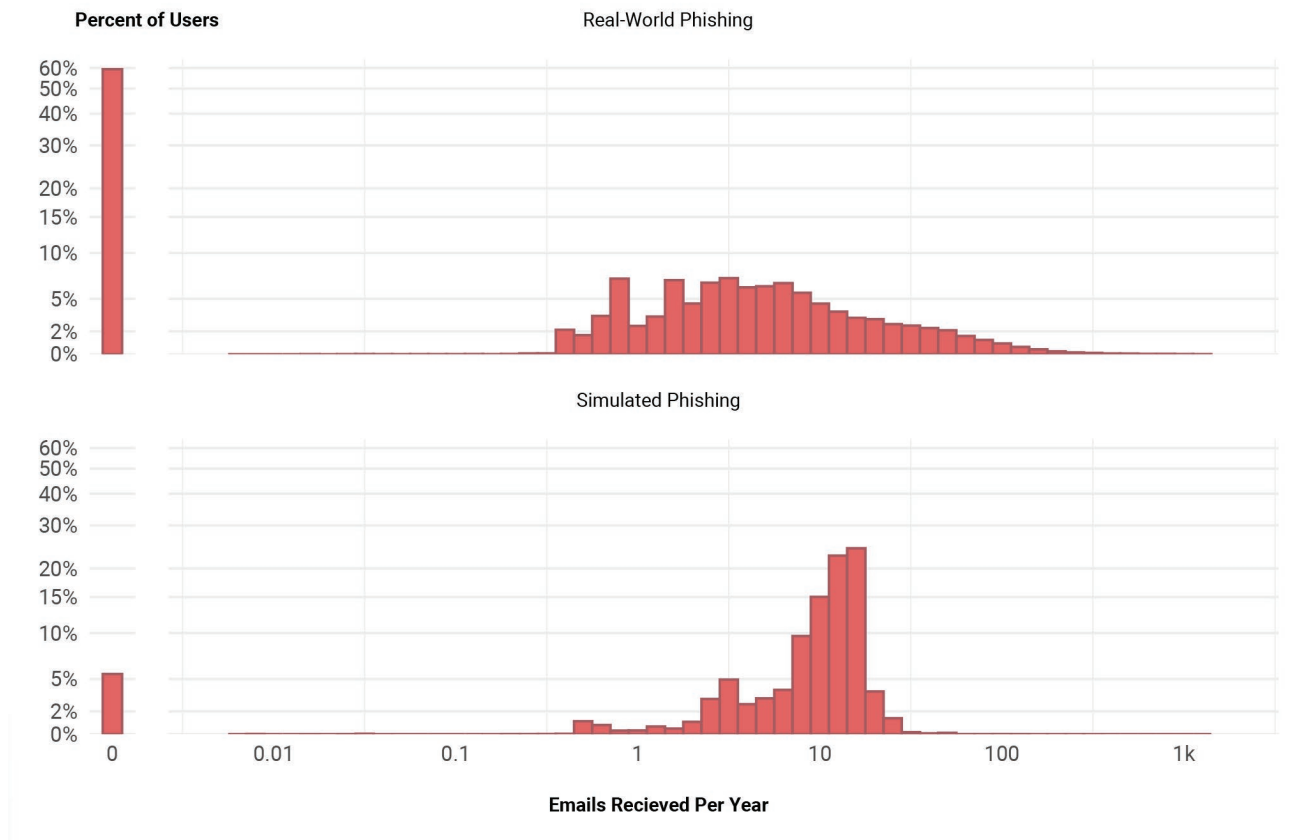


Figure 1: Comparison of phishing emails received per employee per year for real-world phishing and simulated phishing campaigns



We focus only on browsing behavior involving websites known to be the home for various web based attacks.

What harm does visiting a website that isn't legitimate cause?

Users are rapidly bombarded with malware, phishing campaigns, drive-by-downloads, etc.

We can see a few interesting things by looking at the distribution of phishing emails received in a year—both simulated and real. First, some people receive disproportionately more real phishing emails than their peers. In contrast, simulated phishing emails are delivered at more regular rates. This makes sense when we think of this type of phishing as a training/awareness exercise. This pattern can also be a product of a consequential real phishing event occurring that inspires an organization to double down on training programs—simulated phishing emails being one of the primary ways to educate employees on how sophisticated attackers can be.

Malware

Malware events are much rarer than phishing events, both real and simulated. In our current data set, we explored a total of 9,238 malware events, which were caused by 0.8% of users engaging with the malicious software. While both malware events and phishing events can instantly impact organizations, there is some solace in the fact that malware events are less common. Succumbing to phishing attacks can have some disastrous consequences, but it just allows hackers in the door. Malware events allow attackers to “make themselves at home” in your network.

Browsing

While phishing and malware behaviors can immediately impact an organization's network, there is also another risky behavior that users can engage in—browsing the Internet. It's something that every single human on the Internet does, and on its own, isn't inherently risky. However, waiting behind every legitimate website are questionable ones—sometimes even malicious websites that aim to confuse users into engaging with dangerous content that looks “safe enough.” Because of this danger, many organizations enforce browsing and content controls to prevent users from accessing websites that can potentially cause harm.

In our previous report, our data came from each organization's definition of what websites can cause potential harm. This included websites that might be leveraged to compromise a user's machine, and those that are simply “time wasters.” This time around we focus only on browsing behavior involving websites known to be the home for various web based attacks. What harm does visiting a website that isn't legitimate cause? Users are then rapidly bombarded with malware, phishing campaigns, drive-by-downloads, and more.

So, What Makes a High Risk User?

The three risky behaviors above highlight the pitfalls that users are routinely exposed to and tempted by. Does one group in an organization have more risky users than others, and does the role that an individual has have any influence? Since we know that risky users participate in any of the above three behaviors, how can we ensure we focus on the riskiest users in an organization?

For us to take a deeper look at risky user data, we'll have to continue to define what a risky user is. A high risk user is a user in the top quartile (75th percentile or above) of users in their organization who have had at least one instance of risky behavior or event. As in the last report, this is an organization-specific measure—one company's 75th percentile might be one malware incident in a year, while another might be 20. However, since we are interested in finding out where organizations' high risk users are, this measurement allows us to concentrate on the most egregious of them all.

A high risk user is a user in the top quartile (the 75th Percentile or above) of users in their organization who have had at least one instance of risky behavior or event.

Characterizing The Cutoffs Of High Risk

Since this is an organization-specific definition, let's get a little deeper into what the top quartile actually means.

CATEGORY	MEDIAN THRESHOLD	MAX THRESHOLD
REAL PHISHING CLICKS	More than 8% click rate	More than 14% click rate
SIMULATED PHISHING CLICKS	More than 10% click rate	More than 22.2% Click rate
MALWARE EVENTS SECURE	More than 1.2 Events/year	More than 1.2 Events/year
BROWSING EVENTS	More than 3.7 Events/year	More than 177 events/year

Table 1: high risk behavior thresholds

Across the three risky behaviors (phishing, malware, and secure browsing), we can see a large variance in the number of events that constitute both the median and max threshold.

For Secure Browsing events, while the median threshold hovers around 3.7 events per year in an organization, the Max threshold is greater than 177 events per year. However, the trend continues within the phishing behavior—the median and the max threshold of simulated phishing clicks are both higher than that of real phishing clicks. Malware events seem to be the least common risky behavior that risky users take - with both the median and the max threshold being close to the same.

The takeaway here is that the definition of “high risk” is (and should be!) organizationally specific. Each organization has a different human risk exposure by virtue of operating in different industries and having different cultures. We hope the above helps you understand better where your organization falls.

How many high risk users are there?

So, how many users actually cross the thresholds above? For a typical organization, these thresholds result in about 12% of users being categorized as high risk. Since our definition is organization specific, this rate can vary, with some organizations having as few as 5% and others as many as 20%!

If users are high risk in one category, do they tend to be high risk across other categories? Turns out, the answer is “sometimes” and is probably even more organization specific than the definition of high risk user. For now, we’ll stick to high risk in any category that means “high risk”. After all, the attacker doesn’t care how they get in, only that they do.

For a typical organization, about 12.8% of users are categorized as high risk.



For a typical organization, About 12.8% of users are categorized as high risk.

Why we worry about high risk users:

30%

of all real-world phishing clicks

41%

of all simulated phishing clicks

54%

of all secure browsing incidents

42%

of all malware events

Where are High Risk Users Hiding?

Now that we know that the call is most definitely coming from inside the house, it's time to figure out where exactly it's coming from. Understanding where high risk users are in an organization can allow organizations to meet their challenge head-on, while diving deeper into answering the question "why." Do some roles inherently come with more risk and, therefore, have more high risk users by default?

What departments are high risk users hiding in?

When we think about high risk users and what departments they might be in, we might find ourselves quickly jumping to conclusions. Are the employees in IT less likely to engage in high risk behaviors than those in sales departments? The teams advocating for stricter security measures and leading training surely can't be high risk teams, right? Stereotypes about technically savvy or unsavvy personnel can sometimes cloud judgment, so let's look at what the data says.

Most departments are composed of about 10% high risk users, but there is some variation. The top of Figure 2 gives the raw percentages and the bottom shows the difference from IT. However, beyond the median percentage of high risk users, looking at the range of high risk users by departments gives us a clearer picture.

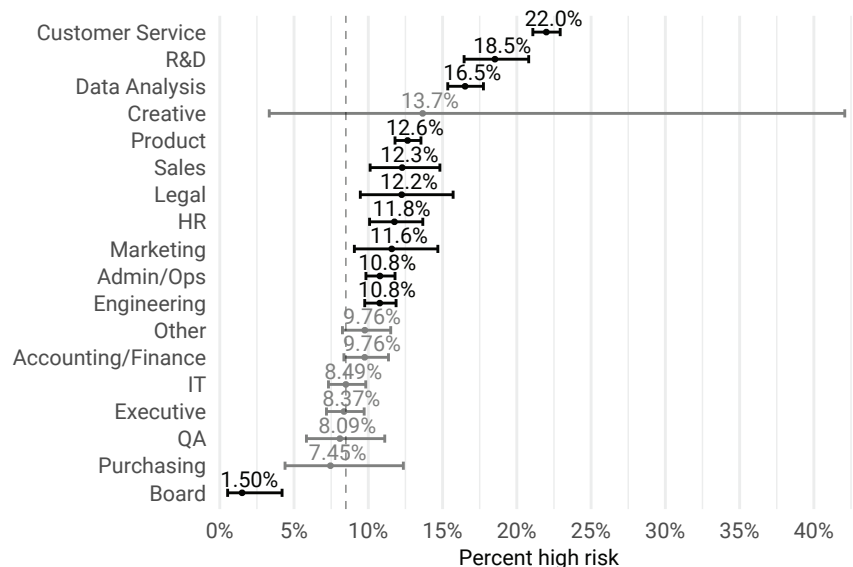
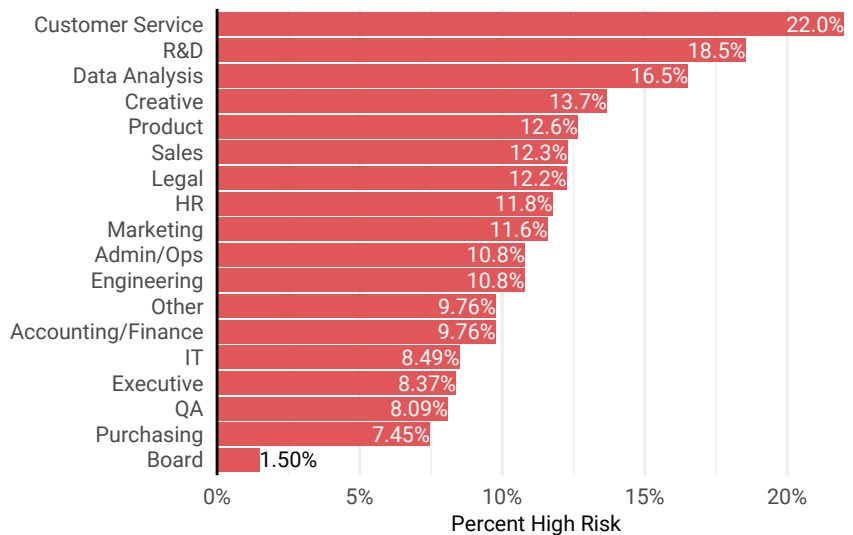


Figure 2 (right): percent High risk by department

So, let's take a moment to compare the rest of an organization's departments to IT, since IT seems to be the barometer that most organizations use for "good users." About 10% of IT department employees are considered high risk users, represented by the dotted line. It makes a clear distinction between those departments with fewer or more high risk users. While the creative department clearly catches our attention, the wide confidence margin has us looking to other departments with a much closer margin—like customer service. Customer relations departments have a marginally higher percentage of high risk users compared to IT departments. Interestingly enough, product departments, along with the executive suite, have a much lower percentage of high risk users compared to IT departments.

The risk differences between these departments might all come down to the behaviors that each of these departments need to exhibit to succeed. Customer relations departments are often responsible for communicating with a wide breadth of users, which may lead to them being exposed to and engaging in more high-risk behaviors. In contrast, product departments tend to be a little more closed off from external dealings. Those external interactions are ripe with the possibility of coming across a malicious site, link, or piece of code. But is there any data to support that hypothesis?

Different Categories Of High Risk By Department

Let's take a look at risk by department. Does one department seem to harbor more high risk users than others? Does the risky behavior exhibited differ based on what department the high risk user works in?

	High Risk Category			
	Malware	Secure Browsing	Real Phishing	Simulated Phishing
Accounting/Finance	0.59%	12.26%	1.09%	10.09%
Admin/Ops	0.46%	13.83%	1.3%	9.41%
Board	0%		0%	9.52%
Creative	0%		0%	14.29%
Customer Service	0%	10.9%	0.09%	19.25%
Data Analysis	0.68%	13.33%	0%	16.55%
Engineering	0.58%	17.63%	0.44%	10.82%
Executive	0%	2.02%	0.37%	6.86%
HR	0.75%	16.43%	1.91%	12.08%
IT	0.24%	17.17%	0.75%	8.66%
Legal	0%	16.86%	1.82%	13.07%
Marketing	3.28%	14.29%	1.7%	15.93%
Medical Lab	0%	21.31%	3.43%	13.45%
Other	0.18%	22.32%	0.94%	10.54%
Product	0%	11.64%	1.12%	0.66%
Purchasing	0%		0%	8.88%
QA	0%		0%	9.25%
R&D	1.99%	19.05%	2.16%	1.08%
Sales	0.16%	1.67%	2.4%	14.51%

Figure 3: Comparison of high risk categories across departments

In figure 3, we see some of those answers start to come out of the woodwork. For example, research and development tends to have the highest rate of events in malware behavior,

while customer service departments have the highest rate of events in simulated phishing. What is important to note is that the highest percentage of risky events happens within browsing behaviors - with lab, research and development, and other, all registering around 20%. Malware and real phishing events seem to happen less frequently across the board. However, that does not mean that they are less impactful events when they do occur.

This implies that organizations should perhaps focus their security resources differently across an organization. Maybe turning up the sensitivity on your phishing detection for the customer service department is warranted (potentially at the expense of missing legitimate communications).

Where in the org chart are they hiding?

The risky behaviors across departments don't quite give us the full picture of where those high risk users really are. Do managers or non-managers tend to be high risk users? Are contractors inherently more risky than full time employees? If we are able to identify where in the organization risky users are, we might be able to gain a little insight on how we can potentially mitigate risk based on organizational location.

Managers

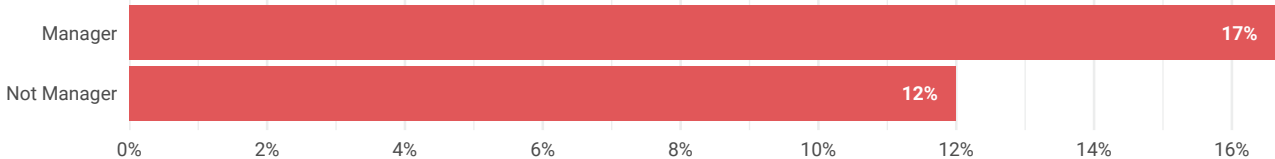


Figure 4: Percent of users that ARE high risk based on whether they are a manager or not

Overall, we only see a slight difference in risk between managers and non managers, with 19% of risky users identified as managers, and 13% as non-managers. Before going any further here, it's important to note that every organization has a different make up of managers and non-manager employees. However, since managers tend to have more access to business critical data, systems, and information, organizations that have a large managerial headcount might want to increase the controls they have in place for this group of authorized users.

Since there is a difference between managers and non-managers, does it matter what department these managers versus non-managers are in, when it comes to high risk users?

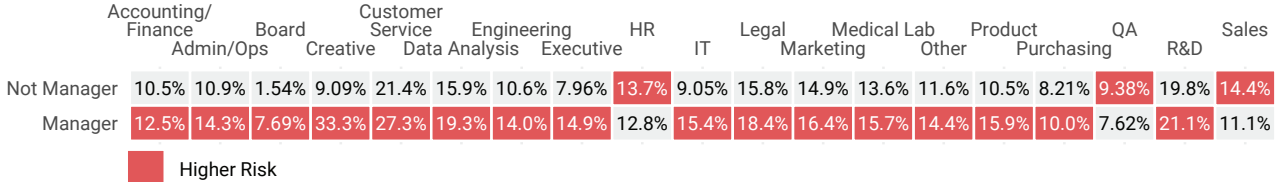
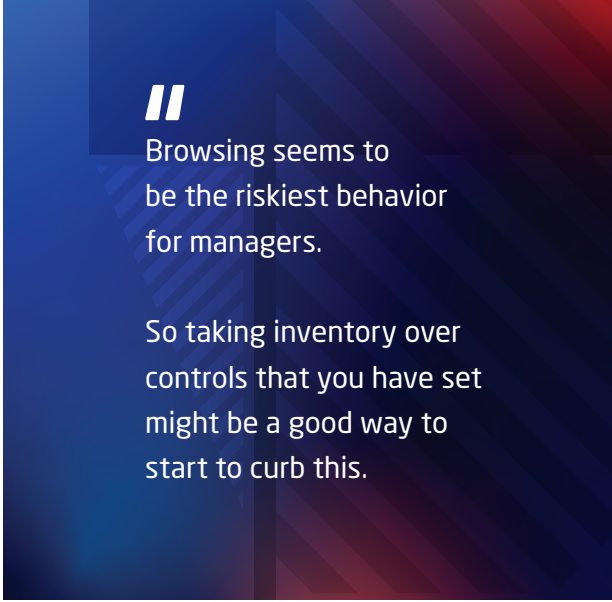


Figure 5: Comparing risk for managers vs non-managers across different departments

It's actually pretty interesting to look at, especially when we think about risky users who are managers and those who are not. For example, high risk users are much more prevalent when looking at managers in the creative department, especially when compared to non-managers in the same department. Creative has the widest gap in high risk users when comparing managerial roles to nonmanagerial roles, while research & development, marketing, human resources, and accounting are all a little closer together. This could be due to how much external collaboration might happen with creative departments. Creative departments often find themselves as a middle point for plenty of projects—handing things back and forth to other teams for approval and then ultimately publication/go live—so this could possibly be one reason why managers in this department seem to be the most high risk. What is interesting to point out, is that the board seems to have the lowest prevalence of high risk users regardless of whether they are managers or not.



Earlier, we talked about the risky behaviors that high risk users participate in, so let's take a moment to also see which of these behaviors managers and non-managers get caught up in.

	Malware	Real Phishing	Secure Browsing	Simulated Phishing
Manager	0.06%	0.74%	6.44%	9.73%
Not Manager	0.08%	0.20%	1.72%	10.04%

Higher Risk

Figure 6: Comparing risk for managers vs non-managers a cross risk categories

By and large, managers and non-managers have higher instances of engaging with simulated phishing events. Secure browsing is where we see the largest difference between managers and non-managers, with an almost 5% difference between the two. Since our data set has already removed legitimate sites that might end up just being a productivity timesuck, like many social media sites, this means that there is a marked difference in how managers and non-managers interact with secure browsing. Malware instances are virtually equal across the board. This observation still lines up with our observations earlier in this report that simulated phishing events are the most common high risk behavior (and event), while malware tends to be the least.

So what does this mean for organizations? Browsing seems to be the riskiest behavior for managers, so taking inventory over the controls that you have set might be a good way to start to curb this. Now that we've taken a closer look at the high risk users in both the manager and non-manager role, let's turn our attention to someone else that companies rely on: contractors.

Contractors

Contractors can often be lifelines for many organizations. They often help fill in the gaps, and assist with business-critical continuity. In a post-2020 world, they are, more often than not, almost as necessary as full-time employees. However, do contractors carry more risk than employees? Are they more likely to be a high risk user for organizations? Logic would tell us “probably”, since they often aren't bound to the same security training, or regulations, that full-time employees typically have.

	Accounting/ Finance	Board Admin/Ops	Board Creative	Customer Service	Data	Engineering Analysis	Executive	HR	IT	Legal	Medical Marketing	Lab Other	Product Purchasing	QA	R&D	Sales			
Not Contractor	12.7%	12.7%	11.8%	15.4%	22.7%	18.1%	12.6%	16.5%	14.6%	12.6%	16.5%	17.7%	14.6%	14.4%	13.1%	8.43%	9.95%	20.9%	14.6%
Contractor	6.91%	5.66%		0.875%	6.38%	4.39%	5.91%	4.01%	4.72%	4.00%	4.17%	3.13%	5.22%	0%	12.5%	3.57%	0%	13.0%	


 Higher Risk

Figure 7: Comparing risk for full time employees to contractors in different departments

In almost all of these cases, except in the sales and purchasing departments, contractors are less likely to be risky users when compared to full time employees. We can see a few unknowns, which is most likely due to the reporting organizations not using contractors who report to those departments (which is most likely the case in research & development, product, and the board), or an oversight in tagging (which is most likely the case when it comes to creative).

The contractors who are working in sales and purchasing give us an opportunity to think about how that department not just interacts with their customers, but how they can also work to keep their contractors safer when dealing with other external entities. It is not uncommon for sales and purchasing contractors to be working and interacting with multiple employees and other contractors at any given time. Each additional touch point that a contractor has is another opportunity for a high risk behavior to take place. While the success of these teams is dependent on their interactions, both internally and externally, having an additional set of controls in place might help curb the amount of extraneous risk.

But before we can talk about what controls would be most appropriate, we should take a look at what high risk behaviors contractors partake in.

	Malware	Real Phishing	Secure Browsing	Simulated Phishing
Not Contractor	0.1%	0.32%	2.97%	11.89%
Contractor	0.02%	0%	0.09%	4.54%


 Higher Risk

Figure 8: Comparing risk for employees vs. contractors across different risk categories

Simulated phishing events, again, are the most prevalent across employees and contractors—with employees almost three times more likely to engage with those emails than contractors. Why would there be such a gap? Since some contractors may work with multiple clients and prospects, there is a high chance that they have developed a sixth-sense around phishing emails. During the pandemic, malicious users preyed on unemployed and self-employed people with phishing attacks geared around employment opportunities and business prospects. So, maybe contractors still have a sour taste in their mouth and have their guard up when it comes to all things phishing. The other reason there may be a gap? Many organizations often have strict controls around their contractors as a general rule.

Secure browsing is much more commonplace in employees, and this could just be due to the nature of a contractor. When someone is an hours-billable worker, any time that is used not working on whatever it is they have been contracted to do, isn't paid. So, for many contractors, partaking in secure browsing high risk activity may not even be something they consider.

Taking it back up to the previous chart, we saw that contractors in purchasing and sales had the highest percentage of high risk users. It wouldn't be out of the question to say that contractors in

those two departments are most likely to engage with simulated phishing attacks, just like employees. So what does this mean for organizations? Maybe give your contractors a heads up that your organization does phishing training (similar to how you communicate it with your employees), and see if the rates go down. It could just be a case of contractors not wanting to miss an email from their client, which then leads them into risky behavior.

Location In The Org Chart

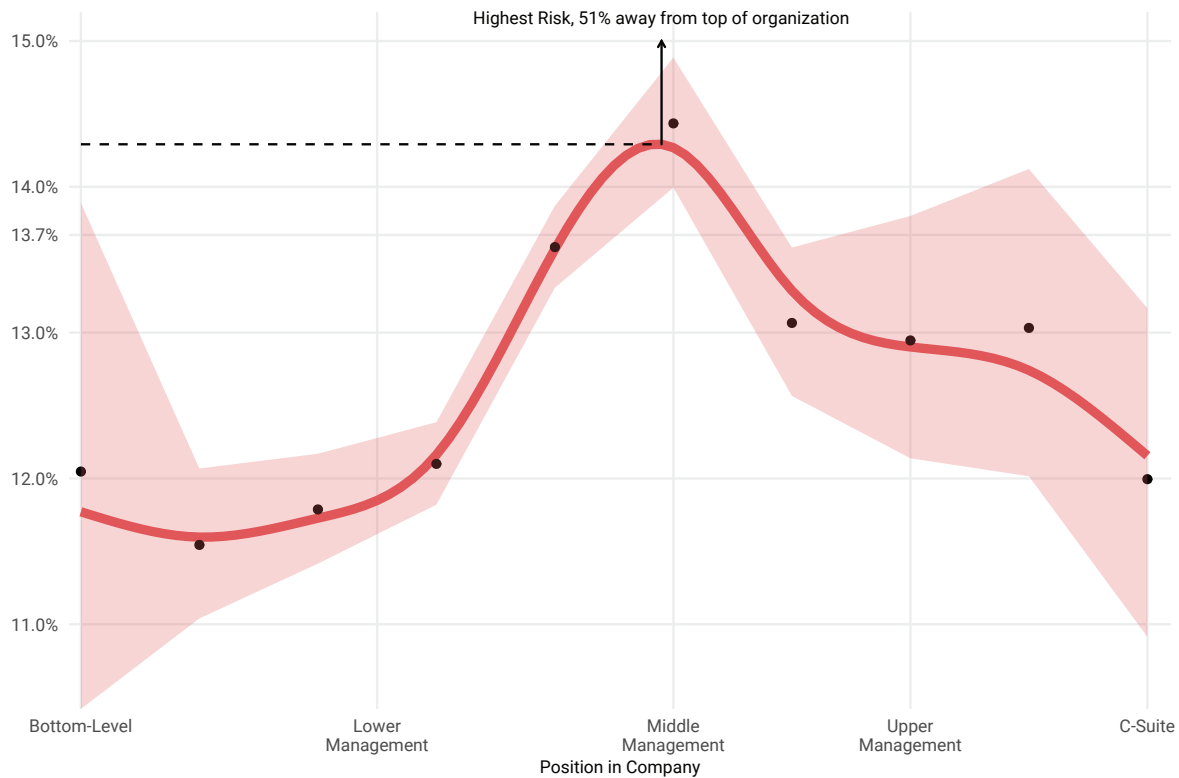


Figure 9: risk by position in org chart

It seems like where you are on the organization chart also plays a small role in determining high risk users. When we take a look up and down the organization chart, measuring the distance that a user is from the top of an organization, we can see that both the top and bottom rungs of an org chart seem to harbor less risky users when compared with the middle.

Does this mean that middle management is riskier? Not necessarily, but it does seem like that part of the organization chart has the highest percentage of high risk users. What it might mean is that the middle of the organization chart has the most people that have the highest amount of touch points throughout the company and with external vendors. If we think about the function of management, they are there to manage a team of employees below them, and then communicate to a team of upper management above them. Then when you mix in the likelihood that middle management may also be in charge of contractors who are helping supplement the work done by their employees, you find the middle swath of your organization flush with multiple risky touch points.

So what does this mean for organizations? The middle of your organization chart packs a powerful punch for business continuity and success. Giving your management teams the support they need can go a long way in helping them limit the amount of touch points they have to interact with, which in turn, may help decrease the high risk behaviors that they unknowingly participate in.

Conclusion

We kicked off this report by asking, “where do high risk users hide in organizations?” The answer to this question seems to be “everywhere.” However, it’s a little more nuanced than that.

Firstly, we looked at high-risk users’ behaviors: phishing attacks (both simulated and real), browsing, and malware. What we found was that the simulated phishing attacks—by and far—outnumber any other type of high risk behavior. What is really interesting, though, is that there doesn’t seem to be a clear correlation between simulated phishing attacks and real world phishing attacks. What appears to be taking place is that organizations are investing in phishing attack training, and high risk users are interacting with them more, maybe because there is just MORE training to begin with.

We found that high risk users are about 10% of each department in an organization, plus or minus a few percent depending on which department they are a part of. While IT is typically the barometer for what many think of as a “low risk” user, when we look directly at how different organizations stack, a few departments have less high risk users than IT.

Beyond the department level, we also found that managers carry a slightly higher percentage of high risk users than non-managers. But, when we looked deeper into which high risk behaviors the high risk users in manager and non-managerial roles took, we found that managers were less likely to get caught up in simulated phishing.

All in all, we know the call is coming from inside the house, but the “who” question seems to be organization specific. Looking at where we found the highest concentration of high risk users may be able to lead you in the right direction. But ultimately, the size and organizational make-up of your organization might influence where your most high-risk users are.

mimecast

Mimecast: Work Protected™ Since 2003, Mimecast has stopped bad things from happening to good organizations by enabling them to work protected. We empower more than 40,000 customers to help mitigate risk and manage complexities across a threat landscape driven by malicious cyberattacks, human error, and technology fallibility. Our advanced solutions provide the proactive threat detection, brand protection, awareness training, and data retention capabilities that evolving workplaces need today. Mimecast solutions are designed to transform email and collaboration security into the eyes and ears of organizations worldwide.

Cyentia Institute is a research and data science firm working to advance cybersecurity knowledge and practice. We do this by partnering with security vendors and other organizations to publish high-quality, data-driven content like this study. Find out more at www.cyentia.co