CLICK ARMOR™
Click With Confidence

CISO REPORT ON SECURITY AWARENESS AND HUMAN RISK MANAGEMENT

HUMAN CYBER SECURITY TRENDS, CHALLENGES, AND SOLUTIONS

Q2 2024

PREPARED BY
SCOTT WRIGHT

Welcome to the second quarter's edition of our 2024 CISO Reports on Security Awareness and Human Risk Management.

Click Armor® summarizes our best insights in each quarter, taken primarily from the words of experts in our bi-weekly Live Cyber Security Awareness Forum (CSAF) panel sessions.

Our live events are held at least once per month, and are announce on LinkedIn, and within our Cyber Security Awareness Forum (CSAF) community. The CSAF site is where cyber security professionals can collaborate to share ideas on how to build a strong and supportive security culture.

Be sure to join the group to participate and hear about the latest events and be notified of posted event recordings.

Red Team Exercises

You've probably heard of Red Team exercises that try to exercise an organization's security. But what value do Red Team exercises really provide for Security Awareness programs?

First: What is a Red Team exercise?

Red Team exercises are like a practice attack on an organization testing the processes, the skills, and perhaps the vulnerabilities of different parts of the organization for management to better understand them.

Why do Red Team exercises?

Red Team exercises provide a realistic threat assessment and doing proactive risk assessments allows us to do proactive risk mitigation. If you see issues during the exercises, you can fix them before you are hit by a real attack. This includes things like fixing your incident response processes which may seem to be well-designed on paper, but which may not always work as well as they can.

Industry Leader-Defined

Challenges

MISLABELLING RED TEAM EXERCISES

"I see a lot of people just calling any type of penetration test or security assessment a Red Team, that's not true at all. A real Red Team engagement is taking a security assessment to the next level. And we really like to talk about real Red Teaming being reserved for organizations that have a very mature security program. We often tell organizations they don't actually need a whole Red Team, they just need a simulation."

-Tom Eston, Snyk

GREY AREAS CAUSING INTERNAL ISSUES

"I've got stories where our Red Team did decide to take things in their own hands and it became more "grey hat" Red Teaming, and it caused some undesirable insider issues that we had to address. Things can get political and out of control very quickly."

-Fletus Poston, CrashPlan

THE THIN LINE AROUND INFORMATION SHARING

"When you are doing really good Red Teaming, there's this weird line where you don't want to inform too many people, but also you don't want to inform no one because then you can run into big issues. You are there to test the system, but you don't want to accidentally break it while you do.

-Jim Guckin, Customers Bank

Solutions

1. Get top-down support.
To tell if your organization is ready for a Red Team exercise, take a look at your executive support. Are they ready and excited to be a part of this exercise? If not, this could be a sign that your culture could use more work before completing a Red Team.

2. Plan rules of engagement thoughtfully.
Your Red Team is going to be completing tasks typically against the organization's policies. Before starting an exercise make sure you check in with your legal, compliance, and security team and nail down: What are you allowing the Red Team to do? What is their change control process? What does their documentation process look like?

3. Alert the correct teams.
Although the purpose of a Red Team is to simulate a real life scenario, there are still certain teams that need to be involved for everything to run smoothly. Communicate with your legal, compliance, and Security Awareness teams as well as your system owners before planning a Red Team.

4. If you can't test, that's a sign.
If you can't test something because it is going to break, that's a sign that it needs to be fixed before executing a Red Team test. Hackers won't stop just because something is going to break down if they scan it. But doing a Red Team test that you know will break something means you likely won't learn as much as you potentially could.

Human Risk Management

There's a growing debate in the cyber security world between the terms *Security Awareness* and *Human Risk Management*. If you've heard of this debate, you may be wondering, "Should I be switching from Security Awareness to Human Risk Management now?" Let's look over the debate:

Concept	Security Awareness	Human Risk Management
Definition	Understanding of security threats, best practices, and policies by individuals within an organization.	Identification, assessment, and mitigation of risks arising from human behavior and interactions.
Context	Key part of a Human Risk Management program	Over-arching program that includes Security Awareness
Focus	Individual knowledge and vigilance.	Holistic approach considering organizational culture, processes, and human factors.
Scope	Primarily individual-centric.	Encompasses organizational and systemic aspects.
Training Elements	Education and training programs.	Integrated risk management strategies.
Outcomes	Improved security practices and incident prevention.	Reduced human-related risks and enhanced organizational resilience.

Cons of adding Human Risk Management

Reasons for not changing program focus and terminology

LOSING PROGRAM MOMENTUM

"Anytime you move in a program within an organization, you're always going to lose traction on your previous program. So it can be: What's the risk/reward here of undertaking this? Are we gonig to lose a lot of momentum that we've built already with a very successful awareness program because all of a sudden we're introducing an HRM program?"

-Ryan Healey-Ogden, Click Armor

POTENTIAL STAFF CONFUSION

Change can be cause confusion around, "Are we replacing Security Awareness with Human Risk Management? Or are we introducing Human Risk Management as an overarching concept that includes Security Awareness? We've been pushing security awareness for 10-15 years, and we're all of a sudden saying "Oh never mind! It's now this!"

-Thea Mannix, Praxis Security Labs

LIMITED RESOURCES TO DO HRM PROPERLY

"There are a limited number of organizational psychologists. There's a limited amount of funding available to do assessments. A lot of organizations are sitting there, without an official assessment of their organizational culture. This is an enormous shift and it's going to be expensive. So make sure you have the right resources."

-Thea Mannix, Praxis Security Labs

Pros of adding Human Risk Management

Arguments for switching to “Human Risk Management”

PRIORITY ON THE HUMAN ELEMENT

“If we are putting ‘the humans’ as our priority piece in the industry, then we need to speak appropriately to the the problem we're trying to solve. The industry has been overlooking the human element in all of this. And so by reframing it, you'll give everybody, including ‘the humans’, a better opportunity to to learn and and make the most benefit from it.”

-Ryan Healey-Ogden, Click Armor

LABELS MATTER

“As a neuroscientist, the argument of, “Why does the label matter?” really frustrates me because I know that what we label things changes our very visual perception of an object. The way that we categorize things and talk about things changes how we view things and it changes the direction of the industry.”

-Thea Mannix, Praxis Security Labs

FOCUS ON THE ENVIRONMENT

“Security Awareness puts focus linguistically on the individual. But we need to focus on the environment. If we want someone to change their behaviours, we shouldn’t go up to each person and try to change their behaviour. That’s time-consuming and costly. Instead, we should change the environment, so they tend to behave the way we need them to.”

-Thea Mannix, Praxis Security Labs

Risk Tolerance in HRM

If you choose to promote Human Risk Management, what does it really mean? And how do **risk management** and **risk tolerance** interact?

Risk Management in Context of Tolerance:
The process of implementing decisions that enable the organization to optimize its level of risk. This includes addressing questions like:

- **Where am I going to spend my next security dollar, and how do I decide that?**
- **What is our current level of risk?**
- **What is our acceptable level of risk?**
- **What happens if someone or something goes out of that acceptable risk?**
- **What threats are relevant to us?**

Bonus Tip:

Three commonly used risk management frameworks for cyber security are NIST CSF, ISO27005 and FAIR.

Challenges

CONFUSING TERMS

"If people not familiar with risk management are puzzled by these terms, it's normal. I've read sources on risk acceptance, risk appetite, and risk tolerance. It can become very complex if you don't have good examples. They can have different meanings to different people."

-Roger Tremblay, Cyber Security Solutions Architect

NOT BEING SPECIFIC ENOUGH

"If you use a methodology and you say, "All high risks are unacceptable," you might want to have some more granularity. You might want to say some risks are more unacceptable than others. So then, you need to choose your risk appetite for certain risks."

-Roger Tremblay, Cyber Security Solutions Architect

LACK OF DATA

"One challenge of using risk management and assessment methodology is the lack of data on these for context. I would try and find better sources of data for these human risk related scenarios. You can try and fine tune your controls based on your understanding of the level of risk, but it can often be a bit of a guessing-game without reliable data."

-Roger Tremblay, Cyber Security Solutions Architect

Click Armor

Solutions

1. Choose a framework and learn the terminology.
Before taking any steps, take the time to learn the differences between risk tolerance and risk appetite and other risk management terms. You can also view this CSAF recording on Risk Management in HRM.

2. Get as much objective data as possible.
Start with assessing your risk levels using objective metrics based on the factors in the framework. Good threat data can be hard to find. Don't just take one, arbitrary source on the likelihood of a threat. Find as much data as you can from reliable internal or external sources to estimate the level of a threat.

3. Get expert opinions.
If there is no data available to you, look for opinions from 4-5 experts on the level of a threat to your organization.

4. Set your standards.
After you know your threats, decide your risk appetite for each. Once you know your appetite, what is your tolerance for these not being met? Doing this will make your risk management program more effective.

Training Your IT Team

We focus a lot on Security Awareness training for all staff. But, what about security training for IT teams? We know there isvendor training for specific technologies, like firewalls or VPNs, but don't forget about the security training IT teams need to understand their roles and responsibilities.

All IT Teams, no matter their expertise in security or tech, should be provided training on a variety of important topics.

IT Team Training Needs

- **Evolving Landscapes**
  - Regulations
  - Policies
  - Workflows
  - Risk frameworks
- **Technical Skills**
  - Cloud computing
  - Cyber security
  - Artificial Intelligence
  - Programming languages
- **Soft Skills**
  - Interpersonal communication
  - Critical thinking
  - Problem solving
  - Adapting

Challenges

OVERCONFIDENCE

“IT teams seem more vulnerable because of over confidence. Experts can get that feelng of, ”I can’t be fooled.” But, every now and then, if you take your eye off the ball, you’re going to have a slip-up. Which in this case, could be your network being compromised.”

-Chris Ellis, Circadence

OVERWHELMED WITH LEARNING

“There’s the vendor training you have to take as an IT professional. That can be overwhelming because some companies have multiple products. And they may be trying to learn multilpe vendor's products. There's just all that hardcore learning of how to use the tools... Not to mention overlaying onto that a consciousness of vulnerabilities and tactics that are evolving out in the marketplace, in the wild.”

-Chris Ellis, Circadence

INSIDER THREATS

“It’s the elephant in the cyber room - insider threats. There are people who make bad lifestyle choices, get themselves badly in debt, and they become vulnerable to being extorted or bribed. They can create a portal in the back door, and then for a handsome amount of cash, provide credentials to someone who wants it.”

-Chris Ellis, Circadence

Click Armor

Solutions

1. Let regular training serve as a reminder.
Have IT Teams take relevant Security Awareness training as a reminder for why it's important to never take the eye off the ball. Include use-cases that show what just one small slip up can cause.

2. Gamify your training.
Add leader boards and other gamified features to increase the engagement, motivation and content-retention of IT teams. Even professionals with deep knowledge in one area need motivation to learn broader security concepts.

3. Allow for practice in a safe environment.
To take away from the risk of learning through "trial by fire", allow your IT Team members to learn through practicing using a simulation environment.

4. Educate on insider threats.
Educate your IT Teams on what bribes and insider threats can look like for IT staff with privileges. Just being aware of the severity of these things can help others stop and spot them before they happen..

Help your team members spot insider threats.

FREE Insider Threat Reminder Card

DOWNLOAD

Combatting fraud aginst employees and customers

Every enterprise has to deal with fraud these days. Many have Anti-Fraud programs dedicated to reducing the amount of unexpected financial loss from fraud. But, these programs focus on fraud against the organization - What about fraud against **employees** as individuals, or against **customers**? These are often forgotten scenarios in any anti-fraud program.

Even if a crime isn't directly targeted at an organization, there are still compelling reasons for why organizations should include them in their program:

AGAINST EMPLOYEES

- Personal financial loss
- Personal stress impacts availability and performance

AGAINST CUSTOMERS

- Large scale financial loss
- Damaged reputation
- High legal costs

Industry Leader-Defined

Challenges

THE RISE OF SOCIAL MEDIA

“You're getting emails, and the attackers are finding out who you are, based on your LinkedIn profile or your social media platform. So it's easy to target you for financial fraud using social engineering, by saying, “Hey, I'm from this company,” or “I'm representing your company.” And convince them to click on a link or take an action.”

-Fletus Poston, CrashPlan

CUSTOMERS AREN’T TRAINED

“The largest risk we see from our customers is them not being able to consume awareness and education in a manner that makes sense to them. Because we have a lot of blue collar workers who might not have formal training on social awareness or Security Awareness at their company. So they really don't understand that side.”

-Ross Bentzler, Alpine Bank

SHOULD WE TAKE ACCOUNTABILITY?

“The accountability side gets to be a little bit more difficult in some ways with the customer side. If you have several 100,000 customers and you're talking about accountability in trying to train all of those customers in a way that they retain that knowledge, that can be relatively difficult.”

-Ross Bentzler, Alpine Bank

Solutions

1. Educate, educate, educate.
Educate your employees on how to assess and verify the source of personal emails, texts, and messages. Teach them the critical thinking skills and questions: Have they reached out to me from this source before? Is this the same tone that they would use?

2. Share as early as possible.
During on-boarding or as early as possible, confirm the emails and platforms you will use to contact employees and/or customers. List the email domains, phone numbers, and platforms you do use along with anything you will never use.

3. Set up reporting processes.
Set up easy reporting processes for both employees and customers to use when they come face-to-face with fraud. Share this process as early as possible, and on a regular basis... and have it easily accessible to both parties.

4. Have a security page.
On your website, have a dedicated page to security. Confirm the official forms of contact for your organization and report any ongoing scams that use your brand name. Also include a form where scams or fraud can be reported by customers.

5. Regularly monitor conversations about your brand.
Use social listening tools like Sprout Social to regularly monitor conversations about your organization. Keep tabs on keywords like “scam” or “fraud”.

Contact Us

We hope you found good value in this Click Armor Q2 2024 CISO Report that can help support your Human Risk Management or Security Awareness program. If you need help implementing any of our recommend tips or ideas, or if you have questions about the identified challenges please connect with us via one of the options below.

Contact Us

Book a Call Here

info@clickarmor.ca