livingsecurity

THE CYBERSECURITY SHIFT:

8 Essential Trends

TRENDING THREATS

Since the 2020 pandemic forced workplaces to transition to a hybrid or remote work model, companies around the world underwent a period of rapid digital transformation. Years later, CISOs are still faced with hardening and improving upon these changes, making strategic adjustments to ensure this new model of working is secure and making it possible to scale in the future.

The lesson in all this is that in times of transition, people, not technology or systems, determine how successful we are at responding to the challenges we face. That's certainly true in the world of cybersecurity, where more than 85% of breaches are caused by human error, action, or inaction. While technology has an important role to play in helping to mitigate organizational risk, the field is shifting to embrace a more holistic approach to risk management, one that addresses the human aspect of risk.

The challenge almost every organization faces with this change in direction is how to objectively solve a problem that inherently lacks actionable metrics. Most enterprise cybersecurity training and awareness programs are lucky to have some basic internal phishing metrics, scores from before and after training, and survey responses that can indicate whether employees enjoyed the training. But what is the impact, did it address the root cause, and does it change behavior?

Human Risk Management solves this problem by applying a previously untapped treasure trove of valuable but disparate data from an extensive array of cybersecurity products. Through automation and intelligent application of timely and engaging cybersecurity-related content that empowers employees, you can turn human risk into organizational strength. Human Risk Management helps security professionals spot both risky and vigilant employee behaviors and gives them the insights needed to measure and demonstrate changes over time, a critical development in the cybersecurity industry.

SOURCE: 2022 VERIZON DBIR REPORT

TREND 1

Employees as Partners, Not Liabilities

Cybercriminals are using an ever-evolving and sophisticated array of tactics targeting employees at all levels of an organization to gain access to their data. While most of your coworkers may say they can distinguish a phishing message from a genuine one, their actions tell a different story. In 2020 alone, the FBI found that over $4.2 billion was lost to cybercriminals. How can you solve for human risk in your cybersecurity equation?

Leverage Human Strength

Regular training is critical in the fight against cybercrime. By simulating phishing attempts to your employees, you can identify who can and cannot spot a well disguised threat. With so many employees working from home, the blurred lines between home and work mean that your security posture depends on human strength more than ever before. Make sure cybersecurity is a top priority for employees no matter where they're working or what device they're using.

While it's tempting to think that additional cybersecurity prevention technology is the answer, the average enterprise has 120 security tools in place. The downside of so many tools is that they send alerts (thousands of them), and your team simply has too many alerts to process. 32% of IT security professionals ignore alerts because so many are false positives. With so many alerts bypassing your security team, you have to turn your end users into your strongest line of defense.

Human Allies

Statistics tell us that people are the problem behind security breaches, but this focus ignores a huge opportunity. When you apply Human Risk Management strategies that transform your employees into your best allies in the fight against cybercrime, your security culture and posture improve dramatically. As we explore in this report, you can arm your people to better identify and respond to threats by using a platform that integrates threat intelligence to meet your employees where they are.

In **2022**, the average
ransomware payment climbed

78%

to an average
$541,000 vs. 2021

SOURCE: PALO ALTO NETWORKS

The Takeaway:

Pandemic-related disruptions to the supply chain, hybrid work environments, and the spread of disinformation have further emboldened cyber criminals. Leveraging the human strength of your organization has never been more important. Empower your employees to defend against cybercrime and they can become agents of detection and prevention.

TREND 2

Move from Disjointed to Integrated

If your approach to cybersecurity technology and processes feels reactive and fragmented, you're not alone. More than half of the executives in large organizations say that the lack of integration between tools is their number one cybersecurity issue. With too many disparate tools and siloed data, it's difficult to correlate trends, identify gaps, and improve the overall security posture.

The Cost of Failing to Integrate

Fragmentation creates the opportunities that cybercriminals are looking for. Cybercriminals are quick to exploit known vulnerabilities associated with specific product settings in your organization's tool stack. We can expect—and should expect—that threat actors will reach our last line of defense. Thus, we must empower our teams with the best knowledge and support we can provide.

Human Allies

To make integration a priority, it helps to have a cybersecurity integration business plan. Run an inventory of your existing cybersecurity tools, analyze how well they work and where your gaps lie, then brainstorm the solutions to integrate, upgrade, and replace as needed. You can use this as a blueprint to identify which systems should share information so that analysts don't have to cross-check multiple platforms. Though integration will likely require a larger up-front lift, the savings in efficiency and ability to demonstrate impact of changing employee behaviors will quickly demonstrate the return in value.

DANIEL J WALSH,
CISO Village MD

VillageMD

"Ransomware gangs and other bad actors, they literally have product teams now that can exploit data leakage opportunities due to lack of integration between tools. This is why reducing human risk is so vital.

Our employees and their patients are forced to keep their head on a swivel, so to speak. We need to elevate our awareness that emails, text messages and even a search result could potentially be a bad actor trying to extract information out of you."

Check out our full interview with Daniel on our blog.

The Takeaway:

Integrate tools where you can across your organization to prevent possible data leaks and exposed vulnerabilities to proprietary content.

TREND 3

Remote Work & The Widening Skills Gap

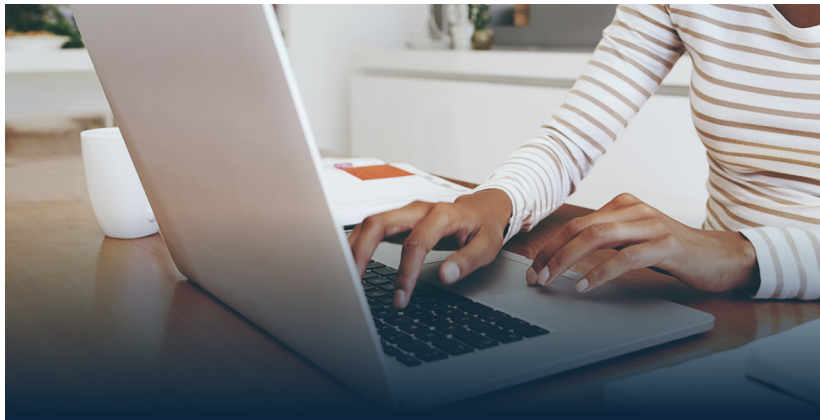
As the pandemic continues to push organizations to digitize their operations to accommodate the growing remote workforce, teams must prepare for an even wider cybersecurity skills gap. Specifically, that remote work landscape provides a fertile opportunity for threat actors to exploit individuals in new ways and there are simply not enough trained cybersecurity experts to keep up with the ever-growing speed and sophistication of cyber attacks.

Social Engineering

Remote work has become an ongoing distraction for cybercriminals to build malicious social engineering attack campaigns. Threat actors have more avenues than ever to exploit these individuals (remote workers have an average of 8 devices connected to their home network). Since individuals spend an average of 58 minutes a day (325 hours a year) on Facebook alone, the vast amount of personal information being shared online makes it easier than ever for cybercriminals to craft convincing attacks & scams for those working remotely.

Building a Company Culture of Security

As threat actors continue to try and exploit remote workers, the amount of job talent available is simply not big enough to meet employer's demand for cybersecurity expertise. To combat the social engineering threat vector, the need for a company-wide culture of security has never been more important. While organizations rush to find help to keep cybercriminals at bay, leaders will need to take a holistic approach to cybersecurity that allows leaders to keep security top of mind across the organization.



> In 2022, leaders will become aware of the hybrid security threat.
>
> Organizations will improve their security operations approach to holistically perceive the threat and move beyond policy/ compliance to security."
>
> SOURCE: MIKE HEREDIA, SC MAGAZINE

The Takeaway:

The need for holistic security awareness training that ensures your entire organization (regardless of cybersecurity expertise) can effectively protect your company from cyberattacks by leveraging your employees as allies has never been more important.

TREND 4

ROI on Human Risk Management

We know human error is the leading cause of data breaches. On the flip side, creating a strong security culture as part of your human risk management strategy is one of the most impactful and cost-effective ways of preventing future breaches. Consider IBM's Cost of a Data Breach ROI calculator, which reveals that 40% of the factors and almost 54% of the financial impact of a data breach can be directly influenced by your cybersecurity awareness program.

Invest in a Secure Future

In recent years, it's become clear that cybersecurity incidents are more influenced by people than they are by technology. The data reveals that more than 82% of breaches are caused by some form of human error, not weaknesses in technical security.

Since people are often connected to cyberattacks, it only makes sense to support and empower them with the knowledge they need to properly defend against targeted threats. As social engineering and other forms of people-focused attacks become more prevalent, your team will become an increasingly important part of your company's defensive strategy.

Take a Pragmatic Approach

Certain departments and individuals on those teams fall into more high risk roles than others. For example, your Finance department is more likely to be targeted in a phishing campaign, since they have access to private information and money. Your C-suite themselves may think they're impervious to cyber attacks, but because of their high privilege and position, they're also routine targets for scammers.

It's up to you to dig into statistics and trust your gut to know who within your company should be considered a greater risk. After determining which members of your organization need to be monitored more closely, it's crucial to keep your focus on them a little more so than others.

Once you've defined the metrics you want to track (here are 6 we recommend), choose a program that makes it easy to manage, access, and analyze that data. With proper analytics embedded into your program, you can easily identify high-risk users and groups, measure return on investment, track behavioral changes, and communicate the results to your most important stakeholders.

The Average Cost of a Data Breach in 2021:

$4.25 MILLION

SOURCE: GOVTECH.COM

The Takeaway:

Define the metrics important to your business, pick a method for tracking them, and analyze, analyze, analyze to demonstrate return on investment (ROI). Once you've determined ROI, proactively use the data to evaluate trends and quickly iterate your program for maximum effectiveness.

TREND 5

Investing in Security Culture

A major impediment to the success of your security awareness program is your employees' perception, and shifting the perception from negative to constructive and encouraging. Security teams are often viewed as the "no" police, there to tell employees what they cannot do and try to catch them making mistakes. Employees often feel unwilling to report potential breaches or risks because they fear the repercussions. At the same time, they may view training as a burden, something that they don't have time for, that is both boring and irrelevant to them.

Taking an Embedded Approach

To create proven and lasting change in security culture, your security awareness training must be inclusive, impactful, and integrated into the culture of the organization. Instead of approaching cybersecurity via a patchwork of band-aid training modules and biannual slideshows, establish cybersecurity as a core value within your company's culture. This ensures that it will remain front-ofmind as your teams encounter threats. As our co-founder and CSO, Drew Rose, likes to say "culture change changes behavior." Ultimately, employees don't make mistakes because they don't care—they do so because they don't understand the impact their actions and decisions have.

Take a Pragmatic Approach

- **Consistent training must be a priority at your organization.** Cybersecurity threats are always evolving and your team needs to be aware of the changes as they occur. There are a number of ways you can boost completion and retention, including experiences that leverage gamification, story-driven training content, and other material that's relevant to everyone on your team.
- **Recruit your people in the fight against cybercrime.** Selling the value of your cybersecurity awareness program can be one of your greatest challenges, but it doesn't have to be. If you can forecast the potential impact of your program, you'll get the company-wide approval and resources you need to implement it. Instead of feeling responsible for vulnerabilities, your team will feel empowered to defend your security—knowing they play an important role in maintaining it.
- **It's not just all about your employee's work life.** All of your employees, no matter what their role is, are interested in keeping themselves and their loved ones safe in the digital world. Our Family First series lets you share content, webinars, and more to help your employees understand how to keep each member of their family safe online.
- **Take it home with you.** If your business has moved to a hybrid or remote-work structure, you need your employees to live and breathe best practices outside of the office too.

Summer Craze Fowler, CIO at Argo AI

ARGO AI

"In the ever-changing cybersecurity threat landscape, it's critical to be intentional about what the need is for the company and whether or not it fits you and your values is just critical. Security is ultimately a part of the fabric of your organization, a part of employees' everyday experience, and something that everyone takes ownership of in their individual roles."

Check out our full interview with Summer on our blog.

The Takeaway:

Make a core company value, like security, a core part of the fabric of your organization, a part of your employees everyday experience, and something that everyone takes ownership of in their individual roles.

TREND 6

Neuroscience-Informed Curriculum

We can all agree that having people sit through a two-hour slide presentation isn't the ideal way to teach them about cybersecurity. That said, how should you educate your employees so they will both remember and be able to implement what they've learned? Here's what science has to say.

Microlearning

"Do you have five minutes to learn about cybersecurity?" According to our biology, that's the working memory capacity and attention span our brains are built to be able to handle in one sitting. This is one of the biggest reasons why microlearning is a growing trend in the cybersecurity awareness space. We can expect this trend to increase and become the predominant training method by 2025.

Storytelling

To create successful microlearning modules, you need to have a main focus or takeaway that supports increased engagement. Who remembers the last test they took in college? Nobody. But everyone remembers the first party they attended. In other words, base the takeaway around a story rather than emotionless statistics and processes. By sharing real and relatable stories about the ways in which people can fall victim to hacks and scams, you can make them memorable. Research bears this out: we're more likely to accurately recall what we learned and to remember it for longer when the information was conveyed as part of a story.

Humor

The good news: your security awareness training doesn't have to be a nonstop laugh fest in order to be effective. However, choosing training that incorporates a little levity will help the lessons stick. Humor activates the reward center of your brain, releasing dopamine, a neurotransmitter that is also associated with attention and motivated learning. Humor not only helps people pay focused attention to what you're teaching, it also helps them recall what they learned. A study conducted by Pew Research revealed that people who watch humor-based news programs like The Daily Show were better able to retain what they'd heard than people who had read the newspaper or watched a traditional news program.

The Takeaway:

Microlearning, storytelling, and humor are three ways to make your training more relevant, enjoyable, and memorable. This is why our production team is continually developing new fun & original cybersecurity training series that are story-driven.

TREND 7

Responsive Training

When it comes to managing your organization's cybersecurity risk, one size doesn't fit all. True Human Risk Management requires that you customize training to meet the needs of different groups, and even individuals, and that you prepare your employees for new threats as they arise.

Tailor Training to the Group

Companies are not homogenous, they typically consist of many different groups of stakeholders, each with differing levels of security knowledge and different behaviors that need to improve. Successful human risk management programs meet users where they are, adapting training to each department's function and level of expertise. For geographically diverse enterprises, this could also mean tailoring content to local regulations and risks.

Tailor Training to the Individual

On occasion, post-training assessments or at-work behaviors reveal that an employee needs additional support around a particular concept. Ideally, your Human Risk Management program should be structured in a way that allows you to deliver targeted training on an as-needed basis. This includes point-in-time (PIT) training, when your employees need it most. For example, you could push a micro-learning module to someone who has just clicked on a simulated phishing link right after it happens, reinforcing the right behavior in the moment.

Adapt to Evolving Threats

The threat landscape is continually changing, which is why the Living Security team provides frequent training programs that cover relevant, topical real-world events as they happen, like the Colonial Pipeline hack and other rampant ransomware attacks. Such "Campaign in a Box (CIAB)" packages come with:

- Customized messages **organized around a unified theme**
- **Kickoff message** for end users to send via email
- **Core blog post t**o link to or republish on your intranet
- **Week-by-week communication guide** with chat messages and email updates

Campaign in a Box

Try Campaign in a Box for free to keep your training up-to-date and topical to improve end user engagement & retention.

Here's a link to our free CIAB covering the December 2021 Kronos ransomware attack as a starting point.

The Takeaway:

Customized & responsive training content helps keep cybersecurity fresh and top of mind. One example is the Living Security series "The Cyber Kitchen", which combines a reality tv cooking experience with cybersecurity training.

View the trailer here.

TREND 8

Holistic Risk Management

Helping your employees develop a security mindset means building security awareness training programs that connect to all areas of their lives, not just the ones that pertain to their jobs.

Cybersecurity Outside of the Office

By taking a holistic approach to cybersecurity training, you can help your employees incorporate secure habits into their personal and work lives. Cyber hygiene becomes second nature, no matter where they are or what they're doing. It means helping employees safely navigate the realities of a work-from-home setup, like routers and network permissions, VPNs, and accessing work information from personal devices. It also means teaching them how to keep kids and other family members safe online and encouraging your employees to share what they've learned with their friends and loved ones. By acknowledging that your employees have lives outside of work, you not only help them cultivate better cyber hygiene across the board but also underscore the importance and relevance of your training.

The Takeaway:

Cybersecurity is about more than what happens at the office; your training should focus on both work and home life to empower your organization to fight security threats in the hybrid working world of today.

CONCLUSION

For security professionals, the cybersecurity landscape is changing, largely for the better. All around the world, companies are embracing Human Risk Management and moving from reactive, disjointed, control and activity-based cybersecurity programs to ones that are holistic, objectives-based, and that see employees as allies, not threats.

As they do, the reputation of security teams will change from volunteer fire brigades and the departments of “no” to champions of employees and strategic partners to the C-suite. In the coming decade, we anticipate that security professionals will enjoy a more prominent role in their companies as executives and boards recognize how essential cybersecurity is—not just to their data but also to their culture. That’s a win, both for security professionals and for the organizations they serve.

HUMAN RISK MANAGEMENT SOLVES YOUR #1 SECURITY CHALLENGE

Living Security’s mission is to help prevent cybersecurity breaches with a human risk management solution that does more than meet compliance needs, it also truly changes behavior. We believe empowering people is the key to ending cybersecurity breaches.

Living Security’s platform is an automated, easy-to-use solution that combines award-winning and innovative training content with security, behavior, and program data to provide visibility into human risk, produce actionable insights, enable targeted interventions and proactive decision making to improve the overall security of your organization.

READY TO LEARN MORE?

Book a demo today to see why organizations including Sony, Target, and JPMorgan Chase partner with Living Security.

Book a Demo Today!

livingsecurity