aci LEARNING

From weakest link to strongest defense.

Smart cybersecurity training can transform workers into a powerful advantage

FROM ! TO !!! 3

JIU-JITSU: TRANSFORM ATTACKS INTO OPPORTUNITY 5

A WIN-WIN FOR EMPLOYERS AND WORKERS 7

WHAT SMART TRAINING LOOKS LIKE 11

BOTTOM LINE: TRAIN OR PAIN 13

From ! to !!!

"The human element continues to drive breaches. Whether it is the use of stolen credentials, phishing or simply an error, people continue to play a large part in incidents and breaches alike."
- Verizon 2022 DBIR[1].

Sound familiar? For years, human error has been recognized as the weakest link in cybersecurity. People doing things they're not supposed to do. Or not doing things they're supposed to do. Study after study points the finger at workers as the top cause of costly data breaches, system attacks and technology hacks in organizations.

If you were waiting for a good-news "however…", sorry. The peril, unfortunately, continues unabated. Just check a sampling of recent reports:

95%

Human error is a contributing factor in 95% of cyberattacks.

IBM Threat Intelligence survey[2]

44%

Insider threat incidents have risen 44% over the past two years.

2022 Ponemon Cost of insider Threats Report[3]

We could go on. And on.

In sad fact, cybersecurity's people problem is worsening. Data and credential theft. Phishing. Ransomware. Malware. All continue to wreak havoc on and over cloud services, email, mobile, browsers, applications and networks. Hybrid and remote work pose new challenges.[4] These include greater use of public wifi, more employee-owned devices, shared workspaces and poor antivirus, password and VPN hygiene, among others.

What's worse, bad actors continue to devise sophisticated new threats. Some now employ ChatGPT and other forms of AI to create "deep-fake" voices and videos meant to trick workers into illicitly sharing information. Healthcare, education, government/military and small business are new favorite targets; manufacturing a perennial favorite. The results are predictable.

The BIG so-what.

The answer to why organizations need to care about this chronic Achilles Heel is obvious. Let's start with money. (You've probably heard these big numbers before. But in most cases, they are much worse.) Security incidents cost companies and consumers a mind-boggling $8 trillion in 2023[5]. Most of the loss is attributable to, yes, human error.

If those figures are too huge to grasp, let's hit closer to home. An insider security incident lasting more than 90 days costs the average large organization $17 million dollars for direct remediation[6]. "Hidden" related costs (like lost productivity and business) can be nine times greater than that! A breach exposes the company to fines, lawsuits and other civil and criminal actions. And no firm's reputation

$4.6 million

Average cost of credential theft to organizations, a 65% increase from 2020.

85 days

Time to contain an insider threat incident, up from 77 last year.

Source: Ponemon Institute

or stock price is improved by becoming a hacking victim.

Even closer still, incidents can have a negative impact on the careers of employees and managers. Justly or not, security and IT leaders and workers and others lose their jobs. Training heads are not immune.

All this is a stark reminder: Human error remains a huge, growing cybersecurity weakness. Until completely fool-proof technology is invented (no breath-holding, please!) or security AI gets really smart, the threat is not going away.

What's going on?

Let's take a quick step back. Why does an employee give protected information to a stranger? Click on a malicious email? Fail to make basic security updates, even if it's part of their job? Reasons vary. But researchers point to a few common causes:

Lack of awareness.
Even today, a surprising number of workers remain fuzzy on basics like changing passwords or not clicking on suspicious emails and links.

Honest mistakes.
Who hasn't accidentally hit the wrong key? Or forgotten to check or update a file protection? To err here is definitely human.

Stress.
A recent study in the Harvard Business Review suggests work pressure and burnout is why employees violate cybersecurity policies.[7] Fears about job security, conflicting family and work demands divert the busy mind. So does a feeling that security takes extra time and energy, which makes people, whether innocently or intentionally, ignore procedures.

Bad intentions.
Less than you'd think. Only about 3% of cybersecurity incidents are caused by workers with malicious or retaliatory aims, the HBR article reports.

Keep these in mind. They provide important clues to the solution: Effective training that meets workers where they're at and elevates personal and organizational power. The first step is seeing the challenge in a new way.

Ju-jitsu: Transform attacks into opportunity.

Organizational leaders typically react to persistent human vulnerability in cyber defense in four ways. Which sounds like you? (Be honest.)

Denial.

"Our technology is pretty good. It's only a problem if something bad happens. Besides, I got bigger issues." Even pros can succumb. Despite causing the most incidents, human error was cited as the top security concern by just 21% of IT respondents[8] surveyed. Sadly (again), they're not alone.

Blame.

The Web buzzed recently with the story of a top executive whose company suffered a serious, human-caused incident. Their response? Blame staffers, who were fired. Some speculated that workers were sacrificed to ensure the company could collect payment from its cyber insurance policy. Suspicions proved correct, and the exec was fired. Alas, throwing employees "under the bus" to protect one's organization or self is hardly an anomaly. Especially in high-stakes security fiascos.

Half-hearted acceptance.

This person goes along with technology education and protection efforts. But, meh. To them, it's more of a checklist item than a real commitment. And that makes them dangerous, due to unwarranted confidence and wishy-washy support for funding and walking the talk.

Embrace.

With head bravely out of … the sand, this leader acknowledges the seriousness of the challenge. They're willing to invest money, time, support and political capital for educating both rank-and-file and technical workers – including (and especially) security specialists and auditors.

Regardless of where you see yourself, there's good news: Leaders at any level can ask a powerful question that can elevate their organization's security game to a new, higher stage.

aci LEARNING

What if cybersecurity's big people problem was really a huge competitive opportunity in disguise?

What if instead of shrinking from a nasty foe's brute strength and incessant attacks you took a lead from the martial arts wisdom of Jiu-jitsu and used your opponent's own energy to defeat them? But how?

Training. Smart training.

Jiu-Jitsu 1:
Start your transformation journey by flipping perspective. Instead of believing that employees have failed the organization, what if the reverse was true? It's time to take responsibility.

Jiu-Jitsu 2:
Continue by considering the grave harm your cyber attacker intends. Feel the anger, the rage at their rotten souls. Remember it could be your head on the line, or people you care about, and all your livelihoods. Then, channel that power into an iron commitment to build security awareness and technical upskilling. You are now firmly on the path to the realization that your employees are your best defense against cyberattacks[9].

Now, instead of seeing their failure, you focus on your shared success. Success that helps to transform vulnerability into strength. Success that brings clear operational and market advantage. Success that shows you are a master of both defense and offense. Success that changes your organization from victim to victor!

WHO'S WITH ME ?

Too soon? Fair enough. Let's look then at the many benefits of moving from denial, blame and half-heartedness to building a knowledge-powered culture that creates a win both for security belts of every color and the dojo itself.

> **"As an industry, we've failed a lot of folks. We don't give them the tools and the understanding of what they're looking at. We need to help all these workers become sensors in the grid, who can let the company know if they see something unusual and do triage. You can't stick your head in the sand.**
>
> **Ben Finke, Co-Founder/CTO, OnDefend. Host, "Be Cybersecure with Ben Finke", ITProTV.**

A win-win for employers and workers.

Most of us are familiar with the old wisdom: “Teach a person to fish and they will eat for a lifetime.” That’s the basic idea here. Instead of just depending on our firewalls, email scanners and other defenses, equipping employees with awareness and skills adds a tough, sustainable protective layer that benefits everyone. You’ll want to look at two interlocking shields.

Security Awareness Training

Security awareness training is just what it sounds like – proactive skilling for new and current employees, especially non-technical workers. It helps them understand why it’s critical to protect the organization from the cyberattacks they’re most likely to encounter, such as phishing and social engineering. It equips people for action by introducing best practices, policies and procedures about what to do when faced with a threat.

There’s plenty of (and growing) proof that good awareness programs are effective “table stakes” to boost an organization’s cybersecurity success.

> **“If people genuinely believe what they do matters to the company, they’ll work hard. When people are having fun in training, they’re engaged. They’re focused like a laser beam. They’ll feel ‘I’m part of the solution.’ It’s going to trickle up into the culture, almost by osmosis. They’ll know they won’t get into trouble for reporting something. And that we’re all in this together.**
>
> **Daniel Lowrie, Security Subject Matter Expert, ACI Learning. Edutainer, ITProTV.**

aci LEARNING

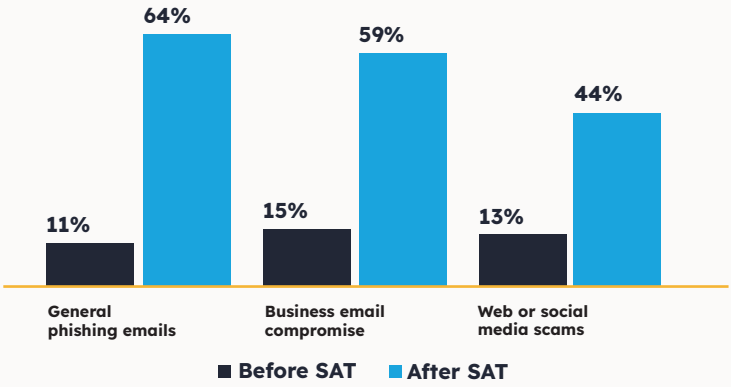
Benefits to workers and employers

Improved skills to defend against common threats.

Take a look at the before and after capabilities of workers who've successfully completed security awareness training (SAT).

The payoff is clear: Trained and aware people have much better odds of thwarting threats, thereby lowering damages and preventative costs. Plenty of research shows workers, boards and the public feel more confident, comfortable and proud of their organization knowing it is secure.

Capability of users before and after training for various threats
Percentage of users viewed as "capable" or "very capable"



Source: Osterman Research, Inc.

Clear ROI to cost-justify expansion of training and hiring security staff.

Effective training pays for itself and can help open the budget doors to continued security education and skilled human fortification. Industry studies show that SAT programs deliver great value.

ROI of security awareness training

	Large organizations		Small organizations	
	Before SAT	After SAT	Before SAT	After SAT
Costs from routine security practices	$5.28	**$4.62**	$29.23	**$21.74**
Costs to remediate major security events	$28.11	**$2.81**	$7.51	**$0.75**
Costs from productivity loss	$455.41	**$45.54**	$249.39	**$24.94**
Costs of a security awareness training platform	$0.00	**$17.50**	$0.00	**$23.00**
Costs to implement an employee training program	$0.00	**$11.90**	$0.00	**$44.61**
Costs to complete training	$0.00	**$27.83**	$0.00	**$21.11**
Total	**$488.80**	**$110.20**	**$286.13**	**$136.15**
ROI	**562%**		**69%**	

Source: Osterman Research, Inc.

A new study[10] by Perception Point/ Osterman estimates security breaches cost the average organization a hefty $1,197 per employee each year. That's the price tag WITHOUT the cost of remediation to address successful cyber incidents across email services, cloud collaboration apps or services, and web browsers. Clearly, money spent on preventative training is a better value than recovering from an incident.

Compliance with security and privacy regulations and laws.

GDPR, SOC 2, HIPAA, FISMA and a growing mountain of industry and government codes[11], including states[12], require various depths of security training. Repeat: It's not an option. The key here, as noted above, is to lean in, not check the box and check out.

A firm foundation for a "security culture."[13]

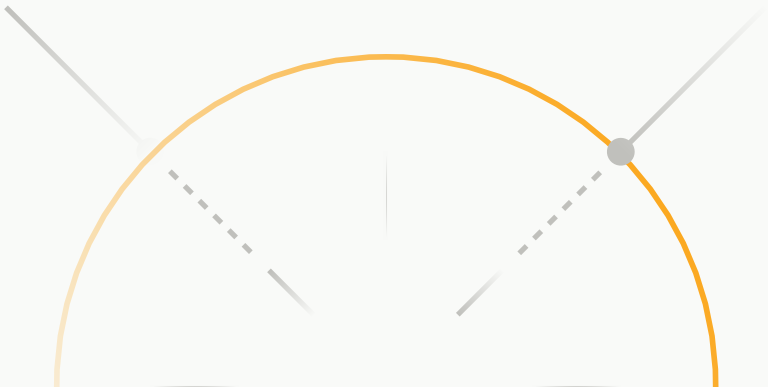
Lots of people today are talking about this. And with good reason. Creating a shared awareness of "that's how we do business here" is an effective way to stop risky behavior and turn every worker into a security sentinel. Meetings, tips and ongoing communication keep momentum. But it starts with an aware workforce and committed leaders.

For more on the benefits of security awareness training, check out this excellent rundown[14] from ISACA, and companion pieces on security vs privacy training[15].

Advanced training and certifications

Cyber attackers are the cockroaches of crime. They adapt endlessly, evolving new ways to pursue their unsavory goals. To fight infestation, security, audit and IT professionals from novice to expert must work hard to keep up with dirty tricks and learn the best ways to stop them. For this, advanced training and certifications on a host of security topics and technologies can equip your ninjas to mount strong defenses and catch-and-kills.

Affordable credentials from COMPTIA, ISACA and other respected industry groups and top vendors are widely valued by employers and employees alike as proof of security bad-assness. CND, CEH, CCNA - the more initials, the badder. Just make sure to distinguish between certifications from major organizations and vendors and less valuable (or worthless) ones from minor or sketchy for-profit granters.



aci LEARNING

Benefits to workers and employers

Valuable in hiring.

Certifications show a worker is motivated and qualified – a boon in helping organizations quickly spot the most qualified candidates.

Improved chances of avoiding, spotting, stopping, managing problems.

That's the point, right? Thanks to effective training, varied organizations saw a 80-95% reduction[16] in phishing, malware and virus attacks, according to Proofpoint, a top security vendor.

Better pay.

A new worldwide industry survey found professionals with cybersecurity certifications earn a worldwide average of $72,244, versus $64,311 for non-certified colleagues. (In North America, the average is $123,370, and proportionally higher than those without.) Other studies report dividends of 35% or more. Yes, as an employer you'll pay more. But you'll get more too.

A key tactic for "Quiet Hiring."

To cope with a competitive hiring landscape, hiring slowdowns and freezes and exhausted workers, many organizations including Google are adopting this new approach. The benefit: employers can add skills and capabilities without adding full-time headcount. Upskilling and moving internal workers into new roles brings employees wanted recognition and growth opportunities, and improves retention. It's a winning strategy that can go a long way in helping to close the IT skills gap[17].

Higher productivity, job satisfaction, retention.

Across the board, workers with certifications report the quality of their work has improved. They're also faster and more engaged. All are proven to increase employee retention. That's a huge marketplace advantage that frees organizations from the cost and time of hiring replacement workers.

Improved customer experience (CX).

Promoting your employee training is a great way to let customers know that you care about and are committed to keeping their data and information safe. It also can open the door to extending your training to them as an important link in the protective chain.

What smart training looks like.

> **The number one thing for smart training is having people with authentic knowledge of what they're teaching. A true expert is passionate and knows the topic intimately. They don't need a teleprompter or a script. They're conversational and can engage the shorter attention spans of today's audiences, and can relate the material to what's going on in the industry today.**
>
> **Don Pezet, CPO of ACI Learning, ACI Learning.**

Pop quiz

Would you rather learn Mandarin Chinese from:
a) 900-page textbook; or
b) Duo Lingo?

Parasailing from:
a) teaching assistant in a lecture hall; or
b) experiential practice.

You get the idea.

Up to this point, we've (hopefully) shown how flipping mindsets and motivations can energize organizations to meet cybersecurity's human problem head-on with better skilling. But not all training is created equal. It's got to be done right!

aci LEARNING

Researchers have shown us that different people learn in different ways. And that different types or modes of training are more effective at certain learning stages. It's no less true with cybersecurity training,

Beat dastardly cybercriminals by copying what they do: constantly adapting to new realities. Here's a checklist of what to look for in a well-rounded, layered, next-gen security training program – one that delivers clear value for today's learners and organizations.

- **Engaging and fun.**
  Busy workers today have high expectations and short attention spans, especially Millennials and Gen Z. People don't want long, boring, stiffly formal lectures. Instead, look for an interactive and conversational style. (Familiar with podcasts?) And who says skilling can't be fun? Infotainment/ Edutainment approaches let people enjoy AND learn. You do not want to get stuck with this guy from 1986[18].

- **Authoritative.**
  Any actor can deliver canned training. Only a genuine SME (subject matter expert, pronounced "smee") has the smarts, confidence and cred to ditch the script and make things relevant, watchable and real.

- **Multimodal.**
  There's no single magic bullet approach. Online, self-paced, instructor-led, video, interactive, community, mentoring. All have different retention rates[19]; all have a place for different learning stages and styles.

- **Hands-on.**
  Real learning takes place by combining head smarts with actual experiences. Your learners - and your training provider - must have both.

- **Customizable.**
  It's an obvious reality: Despite sharing common problems, different organizations have different training needs. One-size-fits-all courses don't cut it. Look for an ability to easily mix and match modules to quickly create a program geared to your specific goals.

- **Measurable.**
  This is a business, after all. Don't work with any vendor that can't demonstrate clear value, including engagement times and exam pass rates. Make them show you.

- **ISO-certified.**
  Make sure your training provider walks the security talk. Certifications from the International Organization for Standardization (ISO) demonstrate independent validation of their commitment to protecting customer privacy and maintaining compliance with global regulations.

- **Always-on.**
  Cybercriminals never sleep. Your training shouldn't either. On-demand learning lets busy workers learn on their own schedule, whenever and wherever.

Finally, two other key things to keep in mind once you've selected a provider. Threats never stop evolving, so training must be ongoing. And while you may be tempted to do it yourself, look carefully at costs. Reinventing the wheel rarely makes economic sense.

Bottom line: Train or pain.

On April 13, 2023, the FBI, NSA and seven international cybersecurity agencies took an unprecedented action[20]. They "encouraged" technology manufacturers to create products that are "secure-by-design" and "secure-by-default." Translation: Don't make customers do all the work, like turning on key protective features and installing safety updates. It's a bold and needed step, but unlikely to happen soon. For the foreseeable future, the burden of managing risk – including and especially human risk – remains on organizations and their people.

How we react to this reality will determine in no small measure how and whether we thrive in an age of unrelenting cyberattacks. It sounds dramatic, but it's true. One good direct hit can be lights out.

Consider two ships: One sails leaky and unprotected among attacking pirates, flogging or hurling clueless crew members overboard after the inevitable trouble strikes. The other has a resolute captain who's always at the ready, backed by seasoned sailors who carry powerful spy glasses and big nets, on round-the-clock watch. Which do you think has a better chance of recruiting crew members? Keeping passengers safe? Beating the other ships to port? Keeping its gold?

Right. Let's get to it.

About ACI Learning

ACI Learning is transforming the way companies train and technology professionals learn across audit, cybersecurity and information technology. Fueling the modern workforce, ACI is trusted by the Fortune 500, leading universities and small businesses alike. ACI is an always-on partner that identifies skill gaps and provides immediate solutions to businesses, channel partners and individuals. From providing technology fundamentals to protecting the systems that send people to space, ACI's credentialed edutainers deliver certification prep and skills training via binge-worthy content that supports all points of the career lifecycle.

For more information, visit www.acilearning.com.

aci LEARNING

Sources:

Page 3
1. Verizon 2022 Data Breach Investigations Report
https://www.verizon.com/business/resources/reports/dbir/

2. IBM X-Force Threat Intelligence Index 2022
https://www.securityhq.com/reports/ibm-x-force-threat-intelligence-index-2022/

3. 2022 Ponemon Cost of Insider Threats Global Report
https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats

4. The Impact of the New Normal on Workplace Privacy, Ponemon Institute/ 3M, June 2021
https://www.ponemon.org/userfiles/filemanager/bkox4uly18udll2ydgyg/

5, 6. 2022 Official Cybercrime Report, Cybersecurity Ventures
https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf?utm_medium=email&utm_source=pardot&utm_campaign=autoresponder

Page 4
7. "Research: Why Employees Violate Cybersecurity Policies", Harvard Business Review, January 20, 2022 https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policies

Page 5
8. 2021 Data Breach Insider Survey, Egress
https://www.egress.com/newsroom/phishing-insider-survey#:~:text=London%2C%20UK%20%E2%80%93%203rd%20August%202021%20%E2%80%93%20Egress%E2%80%99,reporting%20an%20increase%20in%20incidents%20caused%20by%20phishing

Page 6
9. "Your Employees Are Your Best Defense Against Cyberattacks", Harvard Business Review, August 30, 2021
https://hbr.org/2021/08/your-employees-are-your-best-defense-against-cyberattacks

Page 8
10. "The Rise of Cyber Threats Against Email, Browsers and Emerging Cloud-Based Channels," Perception Point/ Osterman Research, Nov. 22, 2022
https://www.prnewswire.com/il/news-releases/enterprises-spend-1-197-per-employee-annually-to-address-increasingly-sophisticated-and-successful-perception-point-301685078.html

Page 9
11. "Security and privacy laws, regulations, and compliance: The complete guide", CSO, May 25, 2022
https://www.csoonline.com/article/3604334/csos-ultimate-guide-to-security-and-privacy-laws-regulations-and-compliance.html

12. 2023 US State Data Protection Laws, International Association of Privacy Professionals
https://iapp.org/resources/article/thompson-hine-2023-state-data-laws-compliance-chart/#:~:text=The%20state%20laws%20covered%20in%20this%20chart%20are%3A,Privacy%20Act%20%28CDPA%29%20Utah%20Consumer%20Privacy%20Act%20%28UCPA%29

13. "The Benefits of Information Security and Privacy Awareness Training Programs", ISACA Journal, 2019, Volume 1.
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/the-benefits-of-information-security-and-privacy-awareness-training-programs

14. "Separating Privacy Awareness From Security Awareness Training", ISACA, March 13, 2023.
https://www.isaca.org/resources/news-and-trends/industry-news/2023/separating-privacy-awareness-from-security-awareness-training

15. "Creating a Culture of Security", Nation Institute of Standards and Technology (NIST), September 28, 2020
https://www.nist.gov/blogs/manufacturing-innovation-blog/creating-culture-security

Page 10
16. "What is Security Awareness Training", Proofpoint
https://www.proofpoint.com/us/threat-reference/security-awareness-training

17. "Everything You Need to Know about the Cybersecurity Skills Gap", ACI Learning.
https://w3.acilearning.com/blog/the-cyber-skills-gap

Page 12
18. Ben Stein as economics teacher, "Ferris Bueller's Day Off", 1986.
https://youtu.be/uhiCFdWeQfA

19. "Choosing The Right eLearning Methods: Factors And Elements," eLearning Industry
https://elearningindustry.com/choosing-right-elearning-methods-factors-elements#:~:text=1%20Self-study.%20Nowadays%20this%20is%20the%20most%20common,...%207%20Simulation.%20...%208%20Game-based%20learning.%20

Page 13
20. Press release: NSA, U.S. and International Partners Issue Guidance on Securing Technology by Design and Default, April 13, 2023
https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3361073/nsa-us-and-international-partners-issue-guidance-on-securing-technology-by-desi/

aci LEARNING

Thank you.

aci LEARNING