Improving Organizational Cybersecurity

What can organizations do to improve their cybersecurity posture?

Educate all employees on security

Protecting the edge is partly about ensuring that the edge users (ie. your employees) are following cybersecurity best practices. These include:

- Ensuring that all passwords are durable and changed routinely
- Using password screen-locking and device tracking for all mobile devices
- Don't give out personal information, usernames or passwords when asked via email
- 46% of cybersecurity leaders target improved security awareness training as something that they would like to invest in if they had more funds available.
- *82% of breaches involved the human element, including Social Attacks, Errors, and Misuse. - Verizon Data Breach Report*

Create Cybersecurity and IT Assistant Positions

Cybersecurity is facing a severe labor shortage. Many jobs go unfilled. Even worse, job stress is causing many employees to leave the field. Not to mention, if your company is hacked into, the stress associated with mediating the breach and recovering data and business operations is sure to lead to employee fatigue, more time off, and/or resignations. Creating new assistant positions:

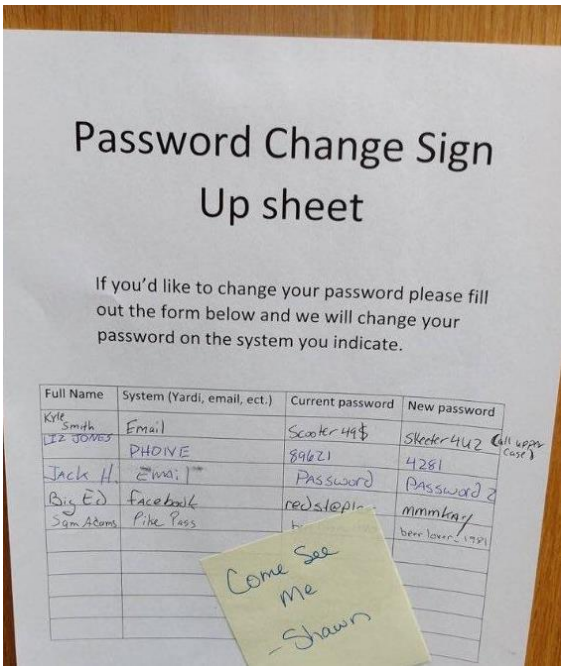
- Allows Cybersecurity and IT employees to assign general office tasks to assistants that do not require a high level of IT or Cybersecurity knowledge
- Allows Cybersecurity and IT employees to be more productive and less stressed
- Allows assistants to develop Cybersecurity and IT knowledge, building human capital in a field that cannot meet hiring demand with jobseeker supply
- Provides for more 'hands on deck' in case of a cybersecurity breach

In November 2018, the InfoSec Institute polled 785 IT and security professionals on career-related questions. When asked which work-related issue keeps them up at night, 12% said they had too much work but not enough staff to help with it all.

Provide IT and Cybersecurity Employees With Wellness Resources

Securing your company's cybersecurity can be stressful, especially at the executive level. The burden of protecting your company's information and operational ability is dependent upon stopping threats that you can't see or hear coming. The 24/7/365 threat of a breach can take an emotional and psychological toll on anyone that works in this field. The best approach for companies to take in order to ameliorate this is a proactive one:

- Encourage Cybersecurity and IT employees to find a counselor or therapist that they can talk to on a regular basis *before* a breach occurs! Both the threat of a breach and a breach itself are stressful events. Having a support network in place beforehand will not only improve employee morale, but also increase employee retention after a breach.
- Provide a short amount of time in the day for Cybersecurity and IT employees to disconnect from job tasks and de-stress. This could be 15 minutes of meditation, breath work, and/or yoga poses. Or it could be 15 minutes of listening to music, or going for a walk outside.
- Encourage employees to use their sick leave! America in particular has a work culture that incentivizes 80 hour work weeks and outworking your peers in order to prove yourself. Create a corporate culture that promotes work-life balance.
- *One-third (33%) of cybersecurity decision-makers are thinking of leaving their role in the next two years due to stress or burnout. -* [*Mimecast Report*]



Have a Plan in Place In Case the Company is Attacked
Creating a security breach plan is useful for a number of reasons:

- Creating a plan is useful because it is a brainstorming exercise that will help you to come up with both better cybersecurity defenses.
- Creating a plan will lead to the identification of choke-points in the crisis response. One example of this is how a breach can often paralyze company communications by shutting down email services, greatly harming company productivity.
- Security breaches are stressful events. Under heightened stress, people have a tendency to shut down neurologically, and critical thinking skills suffer. Having a plan already in place allows taxed decision-makers to have a starting point to fall back on in their response to the threat.
- Not having a cybersecurity breach plan can be incredibly expensive. Businesses with an IR (Incident Response) team that tested its IR plan saw an [average of USD $1.29M lower breach costs] than organizations without an IR team and that don't test an IR plan.

Invest More Money into Cybersecurity and IT Budgets

Cybersecurity suffers from underfunding, and the rise of ransomware attacks has only made the problem worse. Investing more money into upgraded cybersecurity defenses pays for itself:

- 94% of cybersecurity leaders believe more budget is required to combat ransomware, identifying an incremental budget boost of 28% on average
- Nearly two-thirds (64%) of cybersecurity leaders have experienced at least one ransomware attack in the past year
- A single ransomware attack can consume a significant portion of the cybersecurity budget itself. Reaching an all-time high, the cost of a data breach averaged USD 4.35 million in 2022.
- 59% of organizations don't deploy a zero trust architecture. Organizations with zero trust deployed saved nearly USD 1 million in average breach costs compared to organizations without zero trust deployed.
- 46% of cybersecurity leaders say that they need up-to-date security systems.
- Breaches at organizations with fully deployed security AI and automation cost USD 3.05 million less than breaches at organizations with no security AI and automation deployed. 30% of organizations today do not use security AI and automation.