TIP SHEET:

8 CYBERSECURITY STAFFING & TRAINING TIPS
to Turn Your Employees Into a Human Firewall

The 2024 Verizon Data Breach Investigations Report (VDBIR) found that more than two-thirds (68%) of the breaches and incidents analyzed included a non-malicious human element in the attack.

You can reduce your risk and turn your team into a human firewall against cyberattacks by implementing the following hiring and training tips:

1 REFINE YOUR HIRING PRACTICES.

When hiring new employees, consider the 3 Cs of trust: Competence, character, and caring. Ensure you are hiring responsible employees who do the right thing. You should implement strong interviewing practices, check references, conduct regular employment reviews, provide performance feedback, and create a company culture where employees feel their organization and fellow team members care about them and are working towards a common mission with shared values. Creating this environment helps employees feel vested in protecting their organization and team.

2 ESTABLISH A STRONG SECURITY CULTURE.

Internal communication is the cornerstone of establishing a strong security culture in your organization. You need to:

- Start with clear policies that are easy to understand and make sense to employees.
- Have regular internal awareness campaigns throughout the year that not only tell employees what to do to keep the organization safe, but also explain why it's important in terms they understand. When your team understands how an attack can financially devastate an organization, they are more motivated to follow security processes.
- Share examples of the correct behavior and celebrate successes. Praise your team for reporting a suspicious email or verifying unusual requests using a different, known communication method.
- Don't forget to listen to concerns and feedback. Ensure that employees feel comfortable reporting concerns and know that they will not be criticized for reporting an error.
- Consistently apply corrective actions when needed and appropriate.

3 CONDUCT REGULAR CYBERSECURITY AWARENESS TRAINING.

Employees not only need to be competent at their job, but they also need to be skilled at spotting general cybersecurity risks. You should provide regular cybersecurity awareness training for all your employees to teach them how to spot and avoid an attack. Consider managed KnowBe4 training if you wish to outsource the training management function and ensure that a security expert is planning your organization's training modules and schedule. If you plan to manage your cybersecurity awareness training, here are a few best practices you should follow:

- Use micro-stories. Make your training short, relatable, and memorable.
- Engage your audience. Gamification of training can make it more fun and rewarding.
- Make it accessible. Training should be at least monthly, and it's also better if it is on-demand to avoid schedule conflicts and ensure both remote and in-office teams can access the training.
- Keep it current. Ensure the content aligns with today's real-world threats and attack tactics to provide employees with current information so they can spot suspicious activity.
- Use relatable training messages and scenarios. Attendees need to feel it applies to them and understand what to do if they encounter a possible attack.
- Deliver the right training to each segment of your audience. Train your staff and in some cases your customers and community members on how to stay safe. This also requires specialized training for high-risk audiences (finance/accounting, HR, executives, and IT). For more information on role-based training recommendations, read our blog on why cybersecurity awareness training is a top control.

8 CYBERSECURITY STAFFING & TRAINING TIPS

4 IT TEAMS NEED TO STAY CURRENT ON CYBERSECURITY THREATS AND PREVENTION TECHNIQUES.

For example, cloud misconfigurations are a top cause of breaches and very expensive for organizations. Appropriate cybersecurity staffing and training is the best way to reduce your risk. Your team should stay up-to-date on cloud configuration best practices and cybersecurity threat prevention, and regularly audit configurations since they change frequently. There are many free and low-cost training sources such as NIST, ISC2.org, NICCS, Fed VTE, Microsoft certifications, AWS Certified Security Specialist, and many others. You can also find local Defcon and Infosec meetup groups that provide valuable training. If you don't have the time to keep your IT team's skills up-to-date, you can outsource many prevention services. In the example above, you can reduce cloud risks with periodic cloud configuration and security reviews.

5 TRAIN SEVERAL TEAM MEMBERS ON INCIDENT RESPONSE BEST PRACTICES.

Remember general IT teams and cybersecurity teams have different skills and experience. Ensure that several people in your organization are trained to quickly identify and respond to cyberattacks. This can dramatically decrease the financial and reputational damage your organization experiences from a breach. If your team needs training, we offer on-demand Cyber First Responder and Ransomware Response classes to affordably train your team to spot incidents, reduce damages, and preserve evidence to comply with cyber insurance or compliance and regulatory requirements.

6 TRAIN YOUR TEAM USING A TABLETOP DATA BREACH SIMULATION EXERCISE.

Incident response tabletop exercises simulate a breach scenario so you can test your incident response plan for gaps and failure points. IBM's report round that having and regularly testing your IR plan can save you $2.6 million in the event of a data breach. For more information on how to conduct tabletop exercises and our favorite tabletop exercise scenarios, check out our blogs on the best tabletop scenarios for 2024 and evergreen tabletop exercise topics.

7 RETAIN SPECIALIZED LEGAL EXPERTISE.

With new breach notification and cybersecurity regulations from the SEC and FTC, proactive cybersecurity laws in over 19 states and territories, as well as HIPAA, CCPA, and GDPR concerns, you need specialized legal expertise to ensure you stay on the right side of the law and avoid hefty fines and penalties. The most affordable approach is generally to outsource this to a fractional legal resource to determine what laws and regulations apply to your organization and provide guidance on how to comply with applicable regulations.

8 HIRE A CISO OR INVEST IN LESS EXPENSIVE FRACTIONAL CYBERSECURITY LEADERSHIP.

An increasing number of regulators now specify that organizations need a designated, experienced cybersecurity leader. However, CISOs and highly skilled cybersecurity leaders are difficult to find and expensive to hire. In good news, you can hire highly experienced cybersecurity leadership on an affordable, fractional basis to fulfill these regulatory requirements. For more information, read our blog on new regulations and how a fractional CISO can meet that requirement.

We hope you have found these tips on cybersecurity staffing and training helpful!

Please **contact us** if you need support with technical testing, expert advisory services, cybersecurity solutions, or training.

Our expert team is ready to help!

LMG SECURITY

1-855-LMG-8855
info@LMGsecurity.com
www.LMGsecurity.com