The Small Business Imperative

Six Ways to Close the Cyber-Security Gap and Keep Your Employee & Employer Data Safe

isolved®

Cybercrime is on the rise. Companies both big and small are being targeting by bad actors who want to access systems, steal sensitive information and sell it to the highest bidder–and, unfortunately, smaller businesses are even less equipped than their enterprise counterparts to detect, mitigate and respond to risk according to new research.

The World Economic Forum's "Global Cybersecurity Outlook 2024" report found that the distance between organizations that are cyber resilient enough to thrive and those that are fighting to survive is widening at an alarming rate[1]–with preparation levels often driven by company size. Unfortunately for small- and medium-sized businesses (SMBs), the report indicates that lower-revenue organizations are losing more resiliency than gaining it.

Human resource (HR) leaders are heeding the warning. When isolved surveyed HR decision-makers, 41% of them said they are concerned about data breaches this year[2]. While cybercrime is becoming more sophisticated with each passing day, there are several best practices for businesses to incorporate at a bare minimum to keep employer and employee data safe.*

When isolved surveyed HR decision-makers, 41% of them said they are concerned about data breaches this year

[1] https://www.weforum.org/publications/global-cybersecurity-outlook-2024/
[2] https://www.isolvedhcm.com/resource-center/collateral/champions-of-change

1. Build a Human Firewall through Frequent Training

The best defense against bad actors is to educate and enable staff with security best practices. Countless companies exist that will offer mandatory security training to employees that can keep them informed on the latest methods that malicious parties use to gain unlawful access to systems. One source to check out is your company's learning management system (LMS), as most platforms have a large database of security learning. The best systems not only track progress and completion but can communicate to employees about the training and even integrate with the company's scheduling component to make sure employees are compliant before being scheduled to work.

2. Conduct Employee Background Checks

As companies work tirelessly to secure employee data, sometimes it's employees themselves who can be causing undue risk. Employee background checks can help prevent insider threats, verify trustworthiness, identify security risks, ensure compliance and, overall, be a key component in a cybersecurity problem. Today's most trusted human capital management (HCM) systems offer employee background checks in the hiring process and can also intelligently connect to the previously mentioned LMS modules, so information is stored and secured in one system. For any technology, it's critical to work with vendors who prioritize security as mission-critical.

3. Vet Your Platform Partners

The right technology can help you better secure your employee data while others can expose a company to even more risk. When vetting a technology partner to work with, consider:

- Where the vendor hosts their data (i.e., is it on-premise or is it in the cloud and, if so, is it private cloud or shared and through which provider).
- What security and monitoring measures they have in place.
- What third-party audits have been conducted on their processes and platforms.
- Their leadership profile (i.e., do they have full-time leaders in place for key compliance, privacy, risk and security roles).
- And the company's overall innovation and investment in cybersecurity.

Further, if your company has an IT or security team, remember to engage with them early and often for any software implementation project. This will save everyone from not only future risk but also delays of getting the platform live to do its intended purpose.

4. Introduce Administrative Safeguards

Should a cyber-event occur such as a system intrusion by a bad actor or even stolen paper documents from within an office, leadership will have wished they spent more time on training, documentation, practices, policies and procedures. Consider creating a task force to identify current availability of such materials and any gaps that the task force needs to close. Common administrative safeguards include:

- Access control policies
- Employee training and awareness
- Security policies and procedures
- Regular security audits and assessments
- Monitoring and logging of user activities, network traffic and more
- Incident response plan
- Vendor risk management
- Business continuity plans

5. Create Physical Safeguards

Many cybersecurity efforts can appear complicated for those without security backgrounds or training but there are also physical safeguards that most business leaders are aware of–but may not be implementing. Physical safeguards such as security badges, locked doors, access cards, visitor policies, biometric access controls, video cameras, surveillance cameras, motion sensors, fire suppression and environmental controls (e.g., HVAC and humidity controls) can support a company's effort to keep employer and employee data safe.

6. Get Insured

Car insurance is required in most states in the U.S.–it's the cost of driving a vehicle. The same can now be said of cyber insurance for businesses. According to recent data (see sidebar), only 21% of businesses with less than 250 employees carry cyber insurance. This step can support employers with business continuity should an event happen. Savvy companies are considering cyber insurance as the cost of doing business today.

To learn how isolved People Cloud™, the most-trusted HCM platform, protects employer and employee data, scan the QR code or visit https://www.isolvedhcm.com/trust-center

Please keep in mind that employees and employers should never share their login credentials within anyone, including multifactor authentication codes. isolved will never call and ask for this information.

Security Stats to Know

#1 Both cyber leaders and business leaders agree that a gap in resources and skills is the biggest barrier to cyber resilience.

77% Employees who report that their organizations are not cyber resilient, 77% either distrust or are unsure about their CEO's ability to speak about their cyber risk.

21% Not even a quarter (21%) of businesses with 250 employees or less carry cyber insurance.

90% The overwhelming majority (90%) of cyber leaders believe that inequity within the cybersecurity ecosystem requires urgent action.

41% Of the organizations that suffered a material cyber-incident in the past 12 months, 41% say it was caused by a third party.

Via the World Economic Forum's "Global Cybersecuirty Outlook 2024" report.

isolved

isolved®

www.isolvedhcm.com

B0014-1-EN