Webinar 10 – May 22, 2024

Strategies for Managing Technology in the Workplace

WEBINAR OUTLINE

INTRO/SETTING THE STAGE

- Cybersecurity in 2024

WHAT IS CYBERSECURITY?

- Defining Cybersecurity
- Common Types of Cyber Threats
- Benefits of Establishing a Workplace Cybersecurity Program
- Variations of Cybersecurity Measures Among Different Types of Employers

WHY IT IS CRUCIAL TO HAVE A CYBERSECURITY PLAN IN THE WORKPLACE

- Essential Elements of a Cybersecurity Plan
- The Use of Technology Clauses in Employment Agreements

HRtelligence TIPS

WEBINAR CONTENT

INTRO/SETTING THE STAGE

Cybersecurity in 2024

White House Releases 2024 Report on the Cybersecurity Posture of the United States

- On May 7, 2024, the White House's Office of the National Cyber Director (ONCD) released the 2024 Report on the Cybersecurity Posture of the United States
- This first-of-its-kind report provides important updates on how the nation is addressing the challenges and opportunities we face in cyberspace.
- "Simply put, we are in the midst of a fundamental transformation in our Nation's cybersecurity. It is now clear that a reactive posture cannot keep pace with fast-evolving cyber threats and a dynamic technology landscape…"

The Report highlights the significance of cybersecurity and the proactive approach employers should take in response to ever-changing technological developments.

The Importance of Protecting Your Company's Data and Intellectual Property

- Flexible work environments and cloud services have altered how and where your employees can connect and in turn, where your data resides.
- The more spread out your data is, the less visibility and control you have.
- As a result, 66% of organizations have experienced increased security incidents in their remote work environments.

Sources:
https://www.lookout.com/lp/how-to-build-an-effective-data-security-strategy?utm_source=google&utm_medium=search&utm_campaign=GS_AMS-EN_Prospecting_Demand_SSE&utm_keyword=cyber%20and%20data%20security&gad_source=1&gclid=CjwKCAjwl4yyBhAgEiwADSEjeJ4soNkdU2b8nq1wtcVZij1HcieFa8aVTl1krlUKQIbx_NjRxFFF4xoCSHMQAvD_BwE

https://www.ivanti.com/resources/v/doc/ivi/2406/5830d6fdebd2

- Successful protection of confidential information allows the Company to keep staff employed, grow staff opportunities, serve existing customers, and attract new customers.

WHAT IS CYBERSECURITY?

- In the digital age, employers store most information on computer systems and networks. Cybersecurity refers to the technological protection of computers, networks, programs, and systems from attack, damage, and unauthorized access.
- Cybersecurity is particularly important for employers because they maintain a wide variety of confidential information on computer systems and networks that they must protect not only from data breaches that anonymous hackers cause, but also from trade secret misappropriation that their own employees commit.
- With the increasing reliance on technology and digital platforms, protecting sensitive information from cyber threats has become paramount.
- Understanding the role of cybersecurity in the workplace is essential for organizations to safeguard their data and maintain their competitive edge in the digital age.

Defining cybersecurity

- Cybersecurity in the workplace involves implementing strategies to prevent cyber attacks, detect potential vulnerabilities, and respond swiftly and effectively to incidents.
- It encompasses a wide range of practices, including secure network architecture, regular system updates, employee education and awareness, incident response planning, and effective governance.
- Furthermore, the field of cybersecurity is dynamic and ever-changing, with new threats emerging regularly.
- This necessitates a continuous cycle of learning and adaptation to stay abreast of the latest trends in cyber attacks and defense mechanisms.
- By fostering a culture of vigilance and preparedness, organizations can better protect their assets and maintain operational resilience in the face of evolving cyber risks.

Common types of cyber threats

Some common types of cyber threats include malware, phishing attacks, social engineering, ransomware, and distributed denial-of-service (DDoS) attacks.

These threats can result in data breaches, financial losses, reputational damage, and regulatory non-compliance, among other detrimental consequences.

Benefits of Establishing a Workplace Cybersecurity Program

- Establishing and maintaining formalized workplace cybersecurity programs can help minimize the risk of trade secret misappropriation by reducing opportunities for unauthorized parties to gain access to an employer's networks, computers, and data.
- Employers with a well-established cybersecurity program are also better positioned to respond and recover faster in the event of a data breach or trade secret misappropriation.

Notes:
Recovery speed is significant because it shows the employer has an important and protectable interest, which it must demonstrate to a court to establish a trade secret misappropriation claim. Additionally, faster recovery allows an employer to mitigate and limit the damage that may result from a data breach.

Variations of Cybersecurity Measures among Different Types of Employers

- Cybersecurity measures are unlikely to vary significantly based on the type of information that an employer seeks to protect.

Notes:
While a manufacturing company will have different types of trade secrets from a retail company (e.g., blueprints of machines versus customer lists), the electronic storage of trade secrets via a computer, software system, or other online repository means it is possible that they can each be protected by the same or similar cybersecurity methods.

- However, the size of the employer may determine what kinds of cybersecurity measures are appropriate. Certain small companies may have fewer resources and personnel than large companies.

WHY IT IS CRUCIAL TO HAVE A CYBERSECURITY PLAN IN THE WORKPLACE

The Internet allows businesses of all sizes and from any location to reach new and larger markets and provides opportunities to work more efficiently by using computer-based tools. Whether a company is thinking of adopting cloud computing or just using email and maintaining a website, cybersecurity should be a part of the plan.

Theft of digital information has become the most commonly reported fraud, surpassing physical theft. Every business that uses the Internet is responsible for creating a culture of security that will enhance business and consumer confidence.

It is crucial for organizations to have a proactive and strong cybersecurity strategy in place to combat the ever-evolving cyber threats. Companies should adopt a plan to bolster its defenses against the latest cyber risks.

Essential Elements of a Cybersecurity Plan

- Adopt Zero Trust Security

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

- Implement AI Threat Protection

The use of Artifical Intelligence has grown in the area of cybersecurity.

AI solutions can identify shadow data, monitor for abnormalities in data access and alert cybersecurity professionals about potential threats by anyone accessing the data or sensitive information—saving valuable time in detecting and remediating issues in real time.

AI technology also helps identify vulnerabilities and defend against cybercriminals and cyber crime.

- Incorporate Endpoint Detection and Response Solutions

With the rapid increase in remote and hybrid work situations, organizations must acknowledge the heightened vulnerability of endpoints and take immediate action to strengthen their cybersecurity measures. To fortify the cybersecurity plan, it is crucial to implement advanced endpoint protection measures that go beyond traditional antivirus software.

- Create a mobile device action plan

Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password-protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

- Make backup copies of important business data and information

Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Backup data automatically if possible, or at least weekly and store the copies either offsite or in the cloud.

- Employee Cybersecurity Training

Providing regular training sessions can educate employees about the latest tactics used by cybercriminals and teach them how to identify and respond to potential threats. These sessions can cover topics such as recognizing suspicious emails, understanding the importance of strong passwords, and practicing safe browsing habits.

- Regularly Update Systems

Outdated software and unpatched systems are significant vulnerabilities that cybercriminals often exploit to gain unauthorized access to sensitive data. To mitigate these risks, it is crucial for organizations to prioritize regular system updates as part of their cybersecurity plan.

The Use of Technology Clauses in Employment Agreements

The inclusion of mobile device policies and data retention & use policies in employment agreements can act as a safeguard — a tool that delineates how employees interact with and handle your company's sensitive information.

Employees' mobile devices are often insufficiently guarded. By including a mobile device policy in employment agreements, companies define their expectations for the usage of devices with access to company data. These can encompass everything from the importance of regular software updates and the use of secure Wi-Fi networks to the necessity of robust passwords and two-factor authentication.

Companies should clarify what data can be accessed, how it can be used, and how long it should be retained.

Companies should also consider additional technology clauses, such as those related to cloud storage, software use, and social media conduct.

HRtelligence

T TRENDS | **I** INSIGHTS | **P** PRACTICAL GUIDANCE | **S** STRATEGIES

Implementing robust cybersecurity in the workplace offers numerous benefits to businesses and can mitigate the risks posed by cyber threats and gain a competitive advantage in the digital landscape. Some recommendations for employers are, as follows:

Protect sensitive data
One of the primary benefits of cybersecurity measures is the protection of sensitive data such as customer information, intellectual property, financial records, and other critical data must be safeguarded from unauthorized access or disclosure.
Failure to do so can result in severe consequences, including legal ramifications, loss of business opportunities, and damage to reputation.

Maintain Business Continuity
Implement cybersecurity measures such as regular system updates and patches, so that your organization can minimize the likelihood of successful attacks and ensure the continuity of critical processes.

Employee Education and Awareness
Educating employees on best practices, such as creating strong passwords and recognising phishing attempts, enhances the overall security posture of the company.

Conduct Regular System Updates
Regular system updates and patches are vital for addressing software vulnerabilities that can be exploited by cyber attackers. By promptly installing updates and patches, organizations can close potential entry points for malicious actors and ensure that their systems have the latest security enhancements.

Additionally, implementing robust endpoint protection solutions, such as firewalls and antivirus software, further strengthens an organization's cybersecurity defenses.

Set a Cybersecurity Culture

Leaders should prioritize cybersecurity and actively advocate for its importance.

By creating a culture that values and prioritizes cybersecurity in the workplace, companies encourage employees to be vigilant and proactive in identifying and addressing potential cyber risks.

Invest in Cybersecurity Infrastructure

Leaders should allocate resources to invest in robust cybersecurity infrastructure.

This includes implementing advanced security technologies, conducting regular risk assessments, and possibly partnering with reputable third-party vendors.