MARSH JLT SPECIALTY

INSIGHTS | JULY 2020

Why HR Is a Key Stakeholder in Cyber Risk Management

The human resources (HR) function has become integral to organisational cyber risk management in recent years.

Along with information security/information technology (InfoSec/IT), HR is increasingly called upon to help determine and enforce employee data permissions, train and enforce cybersecurity policies and procedures, and help respond to cyber events involving employees.

HR's increased involvement is due to a convergence of factors, including: a more active regulatory environment, the pervasive use of technology and devices in employees' work, and recognition of the importance of a strong organisational cybersecurity culture.

Employees' data and security practices are critical determinants of an organisation's overall cybersecurity. Almost two-thirds (62%) of executives say the greatest threat to their organisation's cybersecurity is employees' failure to comply with data security rules, not hackers or vendors, according to Mercer's *2020 Global Talent Trends Study*.

Yet HR is not typically a primary owner or driver of cyber risk management, as found in Marsh and Microsoft's *2019 Global Cyber Risk Perception Survey*. The great majority (88%) of companies continue to delegate cyber risk first and foremost to InfoSec/IT, followed by the C-suite, risk management, legal, and finance.

This needs to change. A strong partnership between InfoSec/IT and HR is essential for managing data and technology risk, particularly in a remote-working environment.

Below we explore four key areas where the evolving regulatory and cyber risk landscapes are changing HR's role.

Regulatory Compliance

Many regions around the globe and US states are implementing privacy regulations that set strict guidelines for how organisations collect and use consumer data. These include the EU General Data Protection Regulation (GDPR), California Consumer Privacy Act, Illinois' Biometric Information Privacy Act, and the NYSDFS Part 500, among numerous others.

Many of these regulations carry heavy fines, penalties, and the potential for lawsuits, not just for data breaches, but also for improper handling of consumer data. Business leaders recognise the growing risk – ranking regulation/legislation the fourth top risk in our *2019 Global Cyber Risk Perception Survey*.

MARSH

Responsibility for navigating privacy regulatory compliance is increasingly shifting toward HR in conjunction with InfoSec/IT.

HR has traditionally led training on safeguarding sensitive data and the secure use of devices and technologies as part of the onboarding process. Now, HR is also often tasked with conducting privacy regulation training, in conjunction with IT, for employees and for third-party vendors engaging with the organisation's data.

The first two years of GDPR have shown that regulators are willing to impose considerable fines for inadequate data protection, and to hold organisations and individuals accountable for misconduct in data handling.

Determining internal accountability for such errors and misdeeds usually falls under the remit of IT, compliance/legal, and third-party investigators. But given its role in managing employee compliance with organisational policies, HR logically is best positioned to provide guidance on the appropriate punitive or remedial actions for data handling misconduct or errors, as defined by the company's policies.

For this reason, IT, HR, and the C-suite need to be aligned in creating and implementing a robust data incident response plan, particularly for handling events involving employees. This can be aided by agreeing how their respective roles overlap in setting and enforcing data practices and policies, and how the organisation will respond to any regulatory data violation.

Employee Data Controls and Access

Determining appropriate standards for access and controls around sensitive data is a key part of a sound cyber risk management strategy. Here again HR is well positioned to help determine which employee and corporate data is most critical, who in the organisation needs access to it, and how to control this access. Often this is defined when an employee is hired and on-boarded.

This includes assessing whether both current and former employee data – including medical, bank account, compensation information, social security or identification numbers, phone numbers, and home addresses – should be accessible only to certain people for business purposes, or removed from the company's systems.

The end of an employee's tenure at a company is a pivotal moment when HR can play a vital role in supporting sound cybersecurity practices, with advice from the IT team. Several malicious insider cases have occurred after employment was terminated, regardless of whether by mutual decision or not.

HR and IT need to be in sync around the termination process (and mutually agreed departures) so that data access rights are halted as soon as appropriate, usually upon or no more than 24 hours post departure.

Conversely, accidental termination of an employee's ID – for example, due to a miscommunication between HR and IT – can erase emails or documents, and interrupt the employee's ability to work. Such business interruption, if prolonged, can affect the company's performance and revenues.

Data Disclosures

HR also has an important role to play in helping to manage data disclosures and breaches. Whether accidental or malicious, such events can result in significant financial damage, legal action, reputational harm, and loss of consumer trust.

Information disclosures may extend to employees exchanging sensitive information within the office, or remotely around a "virtual water cooler", such as social media.

Data concerning employees located in Europe, California, or other regulated jurisdictions would be protected and subject to regulatory enforcement and/or litigation. Again, it's important for the organisation to have a well-rehearsed cyber and data event incident response plan that involves and defines the role of HR.

In the event of accidental disclosure or a former employee requesting the deletion of their information, best practices call for the incident response plan to define which department would field the breach or deletion notification, which would respond, and what the appropriate response would be. HR is often first to receive such a request from a former employee, and communication and direction with IT and other functions is key to handling it appropriately.

Within most cyber incident response plans, assessing accountability for disclosure events is usually the primary remit of IT, in conjunction with third-party investigators. Again, however, given its role in helping establish and enforce compliance with company policies overall, HR is well placed to provide guidance on appropriate remedial or punitive actions.

A data leak or breach that becomes public knowledge before the company is ready to disclose it or respond, can also negatively affect law enforcement's ability to collect evidence or capture a bad actor.

Whether the disclosure or breach is accidental or malicious, HR policies governing the treatment of sensitive data and employees' social media activities – where those "virtual water cooler" discussions take place – are critical.

Cybersecurity Culture

HR is usually the first (and last) point of contact for employees, and therefore plays an important role in creating and maintaining a robust cybersecurity culture.

Although IT traditionally created cybersecurity training sessions, HR's involvement has increased as the importance of such training for employees has become better understood.

Information provided to new employees about how to practice good cybersecurity hygiene in their daily tasks, can greatly affect their confidence if or when confronted by a scenario requiring them to mitigate a cyber risk.

Training should include guidance for recognising and handling common scenarios, such as phishing and password security. It should also include how to handle the organisation's digital transformation and implementation of new technology, as well as best practices for bring-your-own-device, remote access, business continuity, incident response and recovery, and use of devices.

This training, and enforcement of applicable policies, is very important given that most employees of all levels can now access work emails on their phones and sensitive data and systems from their laptops, starting from day one of employment. The COVID-19 environment makes training and policy compliance all the more critical, given that work-from-home cybersecurity protocols and practices may not be as robust as normal office conditions.

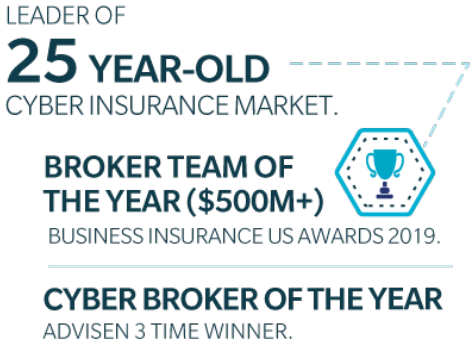
A strong cybersecurity culture must also include consequences for non-compliant behaviour. HR and IT need to collaborate to communicate the ramifications for not following best practice safety procedures, or not completing training – for which more employees are penalised in their performance reviews and even compensation.

In best practice, HR's involvement extends to decisions concerning how to respond if employees repeatedly lose sensitive equipment; how to handle rogue employees who steal sensitive data, but claim it's accidental; and what action to take when notified by employees of a data breach.

These scenarios can be effectively managed if HR is closely involved and updated on the evolving cyber risk landscape and regulatory requirements.

A robust cybersecurity culture starts from the top of the organisation, and involves continuous communication and training for leaders across all key functions. Table-top exercises – simulated cyber events that test a company's response – are highly useful for aligning the actions and priorities of IT, PR, risk management, C-suite, board members, and legal/compliance.

True enterprise cyber risk management programmes include HR in these response testing exercises. Besides HR's important role in cyber risk management planning, its inclusion in event response planning can help align the contemplated treatment of employees with applicable employment regulations and laws, and help mitigate the risk of litigation.



For more information about best practices in cyber risk management, please send an email to cyber.risk@marsh.com, contact your Marsh representative, or contact:

BRIAN WARSZONA
Senior Vice President, UK Cyber Practice
+44 (0) 2073 571544
brian.warszona@marsh.com

Insurance Brokers
Chartered