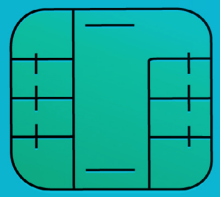
MITRATECH

# Mitigate Cyber Risk with Policy Management



# 01 Mitigate Cyber Risk with Policy Management

Ensuring that employees understand the value and importance of Information Security policies and procedures is critical for information assurance and regulatory compliance.

The tough stance of the UK's Securities and Exchange Commission (SEC) against investment company, R T Jones, offers an impetus for businesses to change their approach to cyber security.

The SEC charged the St Louis-based company with not having data security policies and procedures in place before a cyber-attack from China exposed information on 100,000 brokerage clients.

"50% of the worst security breaches in large organizations are staff related."

**PwC**

R T Jones stored its clients' personal information, including social security numbers, on a third-party web server, which the hackers compromised.

While the company acted quickly, bringing in a cyber forensics team and notifying each client of the breach, the Regulator insisted 'tidying up' was not the point.

The SEC found that during a four-year period, R T Jones failed to adhere to a 'safeguards rule' which requires firms to adopt written policies and procedures reasonably designed to protect customer records and information.

In this brave new world of Regulation and Compliance, it's not just hackers that organizations should fear, but the SEC resolved to punish those that fail to implement sound defenses.

The SEC makes it very clear that preventive measures are vital to minimizing the crippling impact of cyber-attacks in the financial service industry. Andrew Donohue, the SEC chief of staff, warns that the agency will bring enforcement actions against any company's chief compliance officers for looking the other way when it comes to addressing important compliance issues.

All organizations are legally obliged to take appropriate measures to avoid accidental loss or disclosure of information and avoid unauthorized or unlawful data processing or risk regulatory fines.

While organizations know the risks of cyber-attacks, do all their employees? Ensuring that employees understand the value and importance of Cyber Risk policies and procedures is critical for regulatory compliance. According to statistics by leading professional services network PwC, 50% of the worst security breaches in large organizations are staff related, proving that the greatest risk to cyber security is the 'human factor'.

Companies train staff to protect themselves in the real world with health and safety training and all too often overlook the crucial need to teach safety in the virtual world.

"The growing use of social network sites are changing the habits and power of employees and presenting even more challenges to information security."

The growing use of social network sites such as Facebook and Twitter are changing the habits and power of employees and presenting even more challenges to information security.

A rise in the number of people bringing their own devices into the work place is also creating more opportunities for malicious actors to attack organizations through their staff.

Almost half of respondents to a recent Norton survey admitted to not using basic precautions such as passwords, security software or back-up files on their mobile devices.

“One way to demonstrate Best Practice is to implement an industry standard Policy Management solution that adheres to FCPA legislation and ensures a clear compliance audit trail for the benefit of the Board, Senior Management, Auditors and Regulators”

Spear phishing, an email that appears to be from a known individual or business is one way hackers seek unauthorized access to confidential data. The spear phisher thrives on familiarity. He knows your employee’s name, your employee’s email address, and a few personal details. Even the salutation on the email message is likely to be personalized.

A gang of Russian hackers used computer viruses to infect networks in more than 100 financial institutions worldwide, after sending employees emails that appeared to be from a trusted source. Once the email was opened, the malware infected the system allowing the hacker to jump into the bank's network.

Ensuring that employees understand the value and importance of Information Security policies and procedures is critical for information assurance and regulatory compliance.

One way to demonstrate Best Practice is to implement an industry standard Policy Management solution that adheres to FCPA legislation and ensures a clear compliance audit trail for the benefit of the Board, Senior Management, Auditors and Regulators.

Ensuring that employees understand the value and importance of Information Security policies and procedures is critical for information assurance and regulatory compliance.

# Policy Management Software

Policy Management software, such as PolicyHub, ensures the right Cyber Risk policies and procedures get to the right people, that they become accountable by signing up to them and that the entire process is recorded and auditable.

This easy to use and cost-effective software provides a detailed audit trail, reducing the risk of regulatory fines and reputational damage.

Non-technical staff must have an up-to-date awareness of their role in preventing and reducing cyber threats. When carried out effectively, a staff awareness program will help companies identify potential security problems, help staff understand the consequences of poor Information Security, ensure a consistent roll-out of procedures, as well as improve communication between different teams and different levels of the company.

Mitratech's Kristoph Gustovich, VP, Security and Hosting says on the matter:

"One of the top Cyber Security Risks today are specific to the internal threats from employees. Implementing Policy Management software and the security controls associated are now the industry expectation. Utilizing a Policy Management solution that allows for validation of the policies on a set schedule, documentation of employee acceptance, and metrics are just a few of the requirements that cannot be ignored. Cyber-attacks and the methods used by hackers are continually on the increase; organizations need to keep up to date and communicate to all employees, educating them on the latest risks."

# About Mitratech

Mitratech is a proven global technology partner for corporate legal professionals who seek out and maximize opportunities to raise productivity, control expense and mitigate risk by deepening organizational alignment, increasing visibility and spurring collaboration across the enterprise.

With Mitratech's proven portfolio of end-to-end solutions, operational best practices permeate the enterprise, standardizing processes and accelerating time-to-value. By unlocking every opportunity to drive progress and improve outcomes, we're helping legal teams rise to the challenge of serving the evolving needs of the modern, dynamic enterprise.

For more info, visit: **www.mitratech.com**

MITRATECH

## CONTACT US


info@mitratech.com

www.mitratech.com

**Mitratech US**

+1 (512) 382.7322

**Mitratech EMEA**

+44 (0) 1628.600.900

**Mitratech AUS**

+61 (0)3.9521.7077