The dangers within: managing internal cyber threats

Why cyber and technology resiliency is as critical as data security

Risk. Reinsurance. Human Resources.

AON
Empower Results®

The dangers within: managing internal cyber threats

Despite financial institutions (FI) increasingly investing in technology to improve internal controls, staff awareness and threat intelligence, data and systems losses are at an all-time high. Although recent incidents have proved that outside actors remain a major threat, some of the largest losses suffered by financial institutions originate from within, rather than outside the organization. FIs have developed safety measures to prevent and respond to increasingly sophisticated cyberattacks, but cyber and technology resiliency is as critical as data security.

The unexpected risk – perils beyond cybercrime

What should have been a routine system migration for a UK bank in the summer of 2018 resulted in one of the costliest system failure events on record. Sources have reported post-migration costs of £330.2 million (including customer compensation, additional resources, fraud and foregone income). Although this sum was partially offset by the provisional recovery of £153 million from the IT provider, the ongoing reputational damage and backlash from angry customers have made for a difficult recovery. 80,000 customers left the bank throughout 2018 (compared to 50,000 in 2017), with numbers peaking in Q2, just after the incident in April.

"Unlike many other high-profile cyber incidents, the event represents what may be the first business interruption/systems failure claim made to a bank's cyber insurance policy. As such, we're following the outcome of this claim and the markets' response to this claim closely. Meaningful business interruption coverage should be a valuable mitigant in any bank's operational risk and capital management framework, and the sustainability of this coverage feature is critical to this client segment."

Joel Sulkes, Managing Director Global Financial Institutions Practice, Aon

Loss transfer – lessons learned

When financial and reputational integrity rely on digital systems, the enforcement of appropriate safety measures and the creation of a robust cyber risk transfer program are an absolute priority. A regulatory focus in the banking space on capital planning and stress testing exercises has further amplified the importance of managing this type of risk.

Events such as the cyber incident suffered by this UK bank are absolutely insurable. It is vital that risk managers understand that with a robust cyber risk transfer program, the risks associated with internal data and systems risk can not only be managed, but ultimately transferred. With increasing frequency and severity of business interruption (BI) caused by non-physical events occurring in the financial sector, underwriters are appreciating the scope and scale of such losses. Given that coverage has now broadened to include system failures and claims processes have been simplified by fixed deductibles, cyber insurance has become an effective resiliency tool.

The insurance community is following the outcome of this cyber BI claim with great interest, and brokers should be evaluating the sustainability of available products as extremely meaningful risk transfer tools. Non-physical BI can be as critical to the c-suite as the D&O program, and many CROs are now appreciating the importance of broader and evolved cyber coverage.

"Full systems failure coverage should be an integral part of any cyber insurance program. It offers insureds certainty that whatever the proximate cause, the first party loss will be addressed."

Alistair Clarke, Director of Cyber & Commercial E&O, Aon

How can we help

Expertise in identifying and assessing cyber threats is essential in managing changing cyber risks. By using data-driven insights, your Aon team define effective ways to measure performance, and continually develop tailored solutions.

Solution spotlight: business disruption

Aon's cyber insurance solutions contemplate meaningful first party capacity for expense and P&L losses resulting from a breach of security or a failure of your (or your vendors') technology platforms. Coverage may attach at fixed retentions (rather than after waiting period deductibles) and is supported by a partnership between Aon's Cyber Solutions and your line(s) of insurance coverage, which can include:

This collaboration leverages specialist cyber expertise and industry knowledge with a shared focus on supporting the unique characteristics of diversified financial institutions.

Aon's cyber capabilities: expertise and established processes

At Aon, we are united by a shared goal: to protect today and safeguard tomorrow.

Our brokerage and claims teams harness their extensive experience in the insurance marketplace and collaborate with Aon's dedicated cyber specialists to tailor robust planning and incident response capabilities to your firm's needs and objectives.

In 2018, the legacy Stroz Friedberg team formally combined with Aon's cyber brokers to form Aon's Cyber Solutions, a team with more than 650 global professionals dedicated to cyber risk management, cyber security, and cyber insurance.

Stroz Friedberg's experience with high profile breaches over the last decade enables the team to:

We help clients to understand and quantify their risk

- Assess your organisation's security posture
- Align with proven security frameworks
- Proactively test and hunt for malicious activity
- Quantify the potential financial damage from a cyber incident
- Provide prioritised action lists to improve your cyber resilience

We know how to protect an organisation and it's critical assets

- Protect your company from the financial loss of a cyber incident through cyber insurance
- Understand the risks of your investments
- Develop tailored security policies and standards
- Remediate vulnerabilities
- Provide strategic cyber security guidance and develop a programme

We search for the truth and help our clients recover quickly

- Respond defensibly to an attack
- Minimise business interruption
- Use cutting-edge forensics
- Effectively respond to your situation by deploying our team, drawn from the most respected cyber entities trained in the regulatory, financial and legal consequences of a breach
- Help maximise coverage and cost recuperation

By harnessing this expertise in identifying and assessing cyber threats, we support financial institutions to effectively manage changing cyber risks. Aon's cyber team follows a well-established structured process to help you understand and quantify your risks, protect your organization and critical assets, and respond effectively and efficiently to a cyber incident.

Whatever your risk profile, our cyber specialists and FI Practice help you review existing programs, quantify the potential impact of cyber risks and access insurance solutions.

Contact our experts to discuss how Aon can help you build a catastrophe-resilient organization.

Contacts

Joel Sulkes
Managing Director - Global Financial Institutions Practice Leader
+12124412364
joel.sulkes@aon.com

Alistair Clarke
Director & Joint Team Leader - Cyber & Commercial E&O
+44(0)207 086 7357
alistair.clarke@aon.co.uk

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

FP: FP.Global.277.JJ

aon.com

Empower Results®