Executive Summary

Incident Response Challenges and Opportunities for European Enterprises

A CXP GROUP COMPANY

resilient SYSTEMS

Introduction

John Bruce
CEO & Co-Founder

Organisations globally have come to realise that cybersecurity incidents are inevitable, and more costly than ever. Ninety percent of large businesses suffered a data breach last year, according to PwC research.

The impacts of these breaches can be significant — research from the Ponemon Institute shows that the average cost per data breach in the United Kingdom is £2.37m, with Germany and France costing €3.52m and €3.12m respectively. All three countries have seen a meaningful year on year increase.[1] These costs include organisational impact, loss of customer goodwill and the cost of remediation.

What is not accounted for are the additional costs of regulatory fines and compliance. This is a critical factor in Europe, where the introduction of new EU legislation — the **General Data Protection Regulation (GDPR)** and the **Network and Information Security Directive (NISD),** will contain both mandatory breach reporting provisions and fines of up to 2% of an organisation's global turnover for non-compliance. These new regulations, and the growing awareness of the impact to business of data breach, have escalated cyber security to a Board-level discussion.[2]

As incidents are more frequent and complex than ever before, incident response is a daily challenge and increasingly difficult to manage. Whilst companies have historically focused on technology to prevent and detect incidents, it's clear we haven't eradicated the impact of cybersecurity attacks. Today's focus needs to shift to response — building a strategy that recognises security incidents will happen and successfully contends with them. The aim should be to operate with speed and agility, reduce their internal impact, and return to normal operations as quickly as possible.

Businesses are striving for Cyber Resilience and while it's clear we still have work to do, there are encouraging signs that we're heading in the right direction. This change in focus from prevention and detection into response is having a measurable impact.

We recently partnered with Pierre Audoin Consultants (PAC), along with FireEye, HP, and Telefonica, on an independent study featuring 200 recipients from large companies in France, Germany, and the United Kingdom, assessing the current state of cyber resilience in the European market.

This executive summary provides highlights of the full report, which we invite you to download on the **Resilient Systems website here.**

[1] Ref. Ponemon Institute, 2015 Cost of a Data Breach, www-03.ibm.com/security/data-breach/index.html

[2] www.gov.uk/government/uploads/system/uploads/attachment_data/file/385009/bis-14-1277-cyber-security-balancing-risk-and-reward-with-confidence-guidance-for-non-executive-directors.pdf

Key Findings

Huge Gap in Organisations' Perception of Preparedness and Response Plan Readiness

The survey results show that European companies overwhelmingly (86%) feel that they were 'very' or 'somewhat' ready to deal with a cybersecurity incident, with France leading the way at 94%, followed by the United Kingdom at 89%, and Germany at 75%. However, 39% of the organisations surveyed did not have a cyber readiness plan, a number that rises to 52% in France.

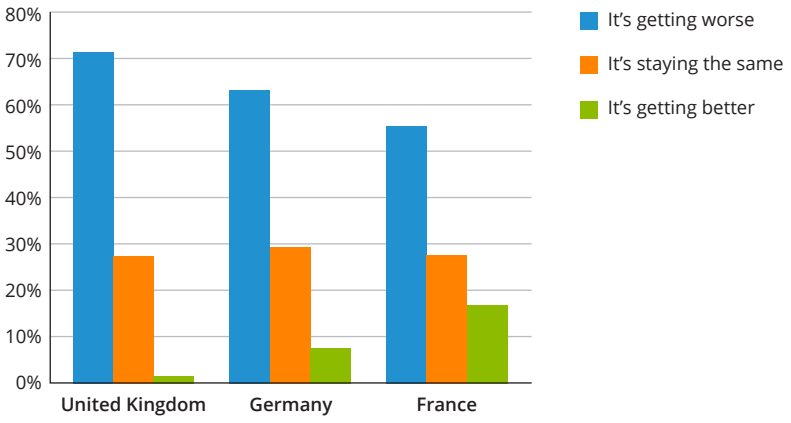
In fact, only 18% of organisations actually have an incident response plan in place, and test in frequently enough to have a good level of confidence in their effectiveness — a long way from the 86% level of perceived cyber-readiness.

Where organisations currently do have a program to test their incident response, the frequency at which they test it is also very inconsistent. Overall, most companies will test their program quarterly (65%), with 5% of firms only testing their preparedness annually — this level of frequency seems insufficient in the fast-moving cyber threat landscape.

The Threat Landscape is Getting Worse—in Terms of Both Volume of Attacks and Types of Attackers

The majority of organisations across Europe (64%) surveyed think that the cyber threat landscape is getting worse, with 28% stating that it remains the same and a surprising 9% seeing improvements in the threat landscape. The United Kingdom had the most respondents who felt that the situation was getting worse (71%), Germany with 63%, and France with 55%.

View of the Cyber Threat Landscape

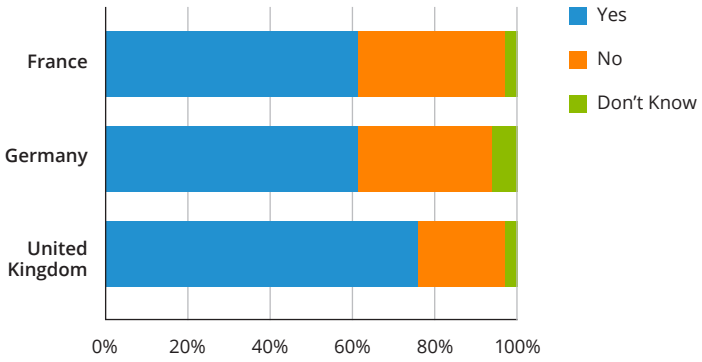


Organisations measured the cyber threat landscape in terms of the sheer volume of threats (74%) and also the type of attackers (66%) — referring to a broad segmentation of nation states, cyber criminals and hacktivists. The potential impact on the business (55%) was also a major consideration, highlighting a more risk-based approach to cybersecurity.

Security Breaches Are More Inevitable Than Ever

100% of organisations surveyed were breached in the recent past — and 67% have been breached the last 12 months. France and Germany had an equal number of organisations breached (62%), with the United Kingdom significantly higher at 76%, of all companies surveyed. This underscores the need for preparedness in response — since it is not a matter of if but when.

Increase in Cyber Security Breaches



These data breach incidents were typically uncovered by the company itself (37%), or by a professional incident monitoring organisation (43%). However, in Germany, 2% of breaches were reported to a company by the media and 21% of the total breaches were reported by a 3rd party. Breaches are typically easier to manage and mitigate if the company itself is in control of the incident, which becomes more difficult when a 3rd party is involved.

Forty-two percent of the incidents were defined as of 'high severity', meaning that the company suffered either a genuine business impact or major internal disruption, with only 23% being considered to be of low severity and minimal impact. Another important finding was that it took the majority of companies between one and six months post-incident to discover the breach, another finding that suggests that improvements could be made in reducing the impact of cybersecurity incidents.

Financial Impact and Recovery Time from Data Breaches is Significant

Nearly 10% of the incidents required direct costs of more than 100,000 euros to mitigate, up to 19% in the United Kingdom. Sixty-six percent of the breaches resulted in costs of between 25,000 and 100,000 euros with Germany reporting the lowest direct costs with no breaches above 100,000 euros and more than a third (35%) at less than 25,000 euros.

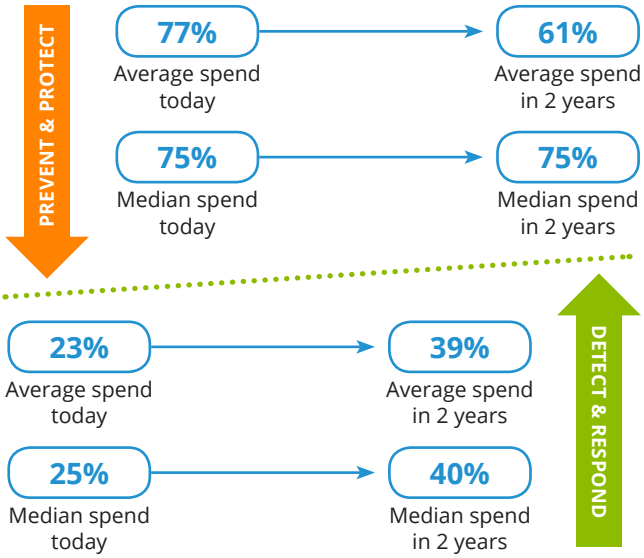
Additionally, firms reported that the majority of incidents took between one and six months to recover from — with 7% of incidents taking between 6 and 12 months. This shows the internal impact that companies are suffering, and is not something that is considered in the direct costs above. Of the organisations that participated in the research, 32% have no policy around data breach notification and 3% have a policy of not notifying customers or regulators — something that will change with the introduction of upcoming EU-wide regulations.

Shifting in Security Spending Towards Response

One of the key areas of the survey is a review on how organisations are spending their information security budgets today, and how that might change in the future. Most companies built their cybersecurity approach around strengthening the perimeter to protect internal corporate resources from attack. As can be seen from the sheer number of data breach incidents, this approach has not worked. Companies are therefore looking at reassigning budget away from 'Prevent and Protect' and shifting towards 'Detect and Respond.'

The good news: companies in France, Germany, and the United Kingdom are shifting their investment focus on how to deal with the outcome of a breach — making sure that they have strategies to detect, manage and remediate cybersecurity incidents. The average spend here will rise from 23% today to 39% in two years. The average spend today across the three countries on 'Prevent and Protect' is at 77%, dropping 16% over the next two years to an average of 61%.

Rising Investment in Response Technology



Organisations Use Make-Shift Solutions to Manage IR

Of the companies surveyed, 61% had invested in commercial software to assist with their incident response strategy.

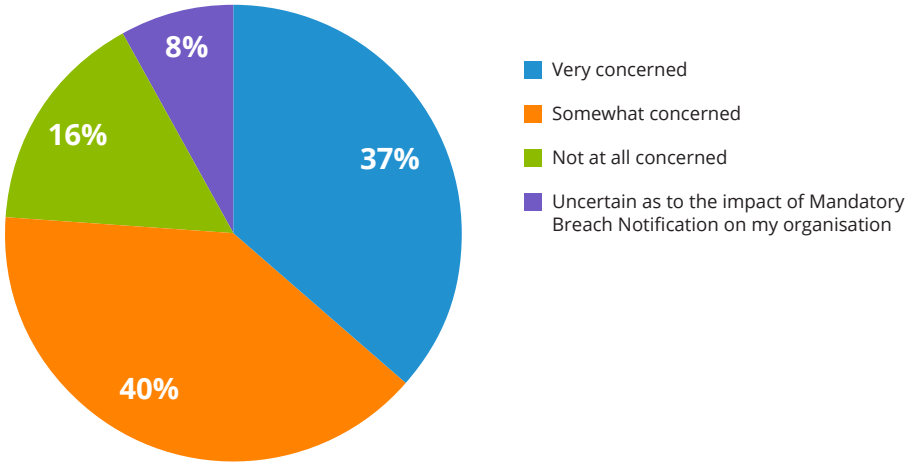
But when you drill into this approach, it seems the largest amount (11%) is spent on developing in-house tools, with others responses referring to associated security technologies such as SIEM, threat monitoring and network security tools. The awareness of the market for specific incident response solutions is not yet where it needs to be — and further customer education is required here.

Strong Awareness of Impending Regulatory Changes

All of the organisations surveyed had some awareness of the upcoming cybersecurity and data protection legislation in the European Union. This is perhaps unsurprising given the large amount of publicity within the information security community in Europe that the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NISD) have received.

As noted elsewhere, both of these have provisions for mandatory breach notification, requiring firms to report all incidents above a certain severity threshold to the regulator. This upcoming regulation is a concern for the respondents, with 77% stating that they are 'very' or 'somewhat' concerned by the prospect. The figures are consistent across Germany (72%) and France (74%), but higher in the United Kingdom (83%).

Growing Concern and Awareness for Regulatory Changes



Conclusion

As the report shows, the volume and severity of cybersecurity incidents continue to rise — and current technology approaches and security strategies aren't enough to address these problems. The challenge for the security organisations will continue to grow — not only is the threat landscape expanding, but the forthcoming introduction of mandatory breach notification at an EU level creates another level of concern.

The key learning is that companies are not sufficiently prepared for cybersecurity incidents. They need to think differently about how they manage cybersecurity within their organisations. It's clear that the approach that we have been using in the past — investing all of our time and resources into trying to harden the network to keep out attackers – is flawed. Companies should accept that focused, well-resourced attackers — whether this is a hacktivist, organised crime or nation-state sponsored approach — can get past any cyber defense.

It's no longer just about prevention — it's about prevailing.

Companies need to take a more balanced approach – combining prevention, detection, and response — to achieve a greater level of cyber resilience to today's threats. Because when incident do occur, security teams will be judged much more on how they manage cybersecurity incidents — and how quickly they are able to detect an attack and roll out an appropriate response.

The good news is that companies are starting to recognise the criticality of response and resilience, and are looking to move investment to how they detect and respond to data breaches. By provisioning their people, process, and technologies for response, they'll empower their teams to quick identify the different areas of risk and regulatory approaches in the countries where they do business — and will be better equipped to react to cybersecurity incidents and minimise their impact on the business.

ABOUT RESILIENT SYSTEMS

Resilient Systems empowers organisations to thrive in the face of cyberattacks and business crises. Resilient's leading Incident Response Platform (IRP) arms response teams with workflows, intelligence, and deep-data analytics to react faster, coordinate better, and respond smarter.

Resilient's security, privacy, and action modules provide organisations with agile, collaborative, and comprehensive action plans — enabling teams to modify responses to suit organisational needs, adapt in real time as incidents evolve, and focus on critical incidents before they become full-blown crises.

Headquartered in Massachusetts, USA, Resilient's customers are some of the world's most trusted organisations.

Learn more at resilient systems.com

ABOUT PAC RESEARCH

Founded in 1976, Pierre Audoin Consultants (PAC) is part of CXP Group, the leading independent European research and consulting firm for the software, IT services and digital transformation industry.

CXP Group offers its customers comprehensive support services for the evaluation, selection and optimization of their software solutions and for the evaluation and selection of IT services providers, and accompanies them in optimizing their sourcing and investment strategies. As such, CXP Group supports ICT decision makers in their digital transformation journey.

Further, CXP Group assists software and IT services providers in optimizing their strategies and go-to-market approaches with quantitative and qualitative analyses as well as consulting services. Public organisations and institutions equally base the development of their IT policies on our reports.

Capitalizing on 40 years of experience, based in 8 countries (with 17 offices worldwide) and with 140 employees, CXP Group provides its expertise every year to more than 1,500 ICT decision makers and the operational divisions of large enterprises as well as mid-market companies and their providers. CXP Group consists of three branches: Le CXP, BARC (Business Application Research Center) and Pierre Audoin Consultants (PAC).

For more information please visit: www.pac-online.com

PAC A CXP GROUP COMPANY | resilient SYSTEMS

Survey Methodology

This survey was conducted by Pierre Audoin Consultants in 2015 with 200 respondents from France (33%), Germany (33%), and the United Kingdom (35%). The majority of attendees were at a CIO/VP of IT level (85%) and all of them were from companies with more than 1,000 employees. The respondents represented 10 different industry sectors, with Government (24%), Financial Services (17%), Education (15%) and Manufacturing (14%) as the most widely represented.

- **GDPR:** The General Data Protection Regulation (GDPR) is the single law to update and unify data protection rules within the European Union. It is a major upgrade to the existing EU Data Protection Directive 95/46/EC, expanding it to cover newer scenarios such as Cloud Computing, Big Data and the transfer of data to non-EU territories. It also includes mandatory breach reporting for all organisations for 'high risk' data and the potential for fines of up to 2% of an enterprise's worldwide turnover or €1m. As of June 2015, this regulation has been approved by the European Council with full EU approval expected at the end of 2015 and member state legislation to come into force by 2017.

  Full text on the GDPR is available here.

- **NISD:** The Network and Information Security Directive (NISD) is the European Union's response to the cybersecurity threat. Among other measures, it requires all EU member states to establish a national network security strategy, with the appropriate regulatory powers to enforce it, and to ensure they have both a national competent authority (NCA) monitor this and a Computer Emergency Response Team (CERT) to handle incidents and risks. It also requires that "market operators" that provide "critical infrastructure" comply with a mandatory security breach and incident notification requirement. As of June 2015, NISD is still under review between the European Council and Parliament. Once passed by the European Commission, all members states will have to enact separate legislation at a later date.

  More information on NISD is available here.

resilient SYSTEMS

200 Brook Drive, Green Park
Reading RG2 6UB
United Kingdom

US +1 617 206 3900
UK +44 (0) 118 949 7555
Fax +1 617 206 3825
Follow Us @resilientsys
Email info@resilientsystems.com

resilientsystems.com

PAC
A CXP GROUP COMPANY

15 Bowling Green Lane
London EC1R 0BD
United Kingdom

UK +44 207 251 2810
UK +44 207 490 7335
Email info-uk@pac-online.com

www.pac-online.com