Accenture
Cybersecurity
Forum
Global

An Overview of Cyber Breaches and UK Cyber Resilience Legislation in 2022

The UK Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, "An Overview of Cyber Breaches and UK Cyber Resilience Legislation in 2022," on May 26, 2022.

Forum members heard from a senior official from the Department of Digital, Culture, Media and Sport (DCMS) about how the government is responding to an evolving threat landscape and then shared their views on how legislation could improve cyber resilience.

This roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers, nor participants, is revealed.

Below is a brief summary of the call:

Change is coming to the ways in which UK enterprises address cybersecurity. Threat actors constantly adapt, technology evolves and regulators work to keep pace. CISOs are advised to watch, listen and prepare.

"Legislation and regulations in the UK are absolutely driving in the right direction," said a subject-matter expert. "The cybersecurity community here is very positive about what is coming out of DCMS."

Cyber Security Breaches Survey findings

The Cyber Security Breaches Survey conducted annually by DCMS explores the policies, processes and approaches to cyber security for businesses, charities and educational institutions. It also considers the different cyber attacks these organisations face, how they are impacted and how they respond.

Among the key findings:

- **UK enterprises are very digitally active:** The vast majority—92% of businesses and 80% of charities—use at least one digital service.
- **Cyber threats are real:** Nearly four in ten businesses and three in ten charities reported a cyber breach in the past year, with phishing the most common.
- **Cybersecurity is more of a priority amongst boards:** It's now at its highest level since the survey started in 2016. However, qualitative findings suggest a low level of expertise amongst boards and senior leaders, which poses challenges.

- **Cyber hygiene is good:** This is particularly true among large and medium-sized businesses. Technical controls such as access management, malware detection, firewalls and data security protections are commonplace.
- **Cybersecurity is recognized as important:** That is, it's seen as being in the interest of customers and service users.
- **Internal expertise is a main challenge**: Also, cybersecurity is often approached reactively, as a cost rather than an investment.
- **Only a small minority of businesses monitor supply chain risks:** This is considered a key vulnerability.

Impact of regulations: Improvements on the horizon

Security of Network & Information Systems (NIS) regulations, currently require cloud services providers, online search engines and online marketplaces to ensure cyber resilience. A recent post-implementation review of impact of these regulations indicates that they have accelerated security improvements among essential services providers in important ways, including:

- 71% of respondents reported increased board support for cybersecurity.
- 71% of essential services respondents reported an increase in board support for cyber security.
- 28% of operators of essential services said they introduced new policies and processes since the inception of the regulations; 51% reported that they updated or strengthened existing processes.
- 54% of digital service providers said it was not easy for them to identify that their organisations are in scope, therefore raising issues about registering with the Information Commissioner’s Office (ICO).
- 9% of essential services operators indicated having the resources to manage the risk from their direct suppliers and their wider supply chain.
- Competent authorities receive little or no reports, suggesting incident reporting thresholds are too high.
- Use of enforcement tools by regulators is lower than the reported need.

The review also identified seven broad areas of improvement:

- Digital Service Providers (DSPs) find it difficult to know whether they are affected by the regulations and thus whether they should register (meaning not all DSPs have been identified).
- Current coverage of the NIS regulations is not sufficient to cover all the risks to the economy and critical services.
- Organisations face difficulties managing the risk from their supply chains.
- There is a lack of funding and/or investment in improvements, and there are challenges securing the right cyber skills.
- Incident reporting thresholds are too high. Regulators not using enforcement tools as often as needed.
- More centralised coordination of NIS implementation is needed across sectors.

Legislation on the horizon

DCMS has consulted on updating NIS legislation this year, and will be publishing a response in the summer. As part of this, Government will ask for the power to amend legislation in the future to allow legislation to keep up to date with changing threats.

Part of the proposal is to expand the regulations to include managed service providers. "When you look at where cyber attacks occur, managed services are increasingly becoming targets," said the DCMS representative. This is a trend that regulators are catching on to. For example, the EU is specifically addressing managed cybersecurity providers."

A second measure aims to address systemic dependence on a handful of critical digital services by proposing more proactive regulatory supervision for the most critical DSPs. Other proposals are intended to ensure the security of supply chains, improve incident reporting requirements and ensure regulation costs are fully recovered by allowing competent authorities to raise fees for all relevant NIS activities.

A **Product Security and Telecommunications Infrastructure** (PSTI) bill aims to bolster the security of IoT connections by introducing three key security requirements through secondary legislation and through an appointed enforcement agent covering new consumer internet and network-connectable products. Regulators note that cybersecurity is an afterthought for many manufacturers of these products. In 2016 there were 13.3 million IoT connections in the UK; by 2024, this is estimated to increase to 156 million.

UK CISO perspectives

Many CISOs endorse regulatory revisions. For example, a Forum member said data protection is critical in thwarting attacks on the supply chain. Said another, "We welcome more scrutiny. It gives me more leverage with the board of directors and helps me make the case for additional cyber investments." Added another Forum member, "Regulations give us a reason to invest in cyber and build new resiliency capabilities." A subject-matter expert said: "We are very supportive of the work DCMS is doing."

Government must find a balance in promoting compliance. When it comes to reporting incidents, "Currently, regulators can levy fines at a high level but that stick may not always be the right tool," said a CISO. "Carrots, and businesses and regulators working together, seem to be effective in promoting compliance with a cyber assessment framework."

Action-oriented regulations are preferred. Rather than simply issuing checklists (which management happens to like), CISOs prefer regulations that call for specific investments such as having a CISO, cyber insurance, an incidence response team on retainer or a threshold of incident response capability. The official from DCMS said: "We don't want to drive enterprises toward a checklist culture. We're trying to avoid being focused solely on compliance."

Overlapping or conflicting regulatory requirements are a cause for concern. "Compliance is becoming quite complicated, particularly for multinationals," said a CISO. "Legislation, regulations and contractual requirements often overlap and make it difficult for us to make certain we're doing the right things." For example, incident reporting time frames range from 24 hours in the EU to 72 hours in the UK.

Short and long-term perspectives. A UK financial services cybersecurity leader said: "We're already feeling the pressure from our regulators to comply with third-party data security requirements and even involve them in our penetration testing. But beyond immediate concerns, subject-matter experts noted that in forums such as Davos and the G7 leaders are taking a longer view of cybersecurity challenges. "There was recently a G7 meeting where they didn't just say cyber is important," said a subject-matter expert. "There was a whole day devoted to cyber resiliency, how do we share threat information and how do we build that longer term capability."

Data misuse among UK agencies not an immediate cause of concern. Unlike in the US, where enterprises worry that cyber incident reporting to one agency might be used by another agency (i.e., the Internal Revenue Service) to take punitive action, UK executives are confident that misuse won't be a problem. "I'm not aware of any incidents where one agency used information in a punitive fashion," said a subject-matter expert. "But as more companies come into the regulatory fold we can't necessarily rely on the close public/private relationships we have today so we may have to look at a more structured approach (to data security.)

A cyber talent shortage is affecting both the public and private sectors. The DSMC representative noted a shortage of 14,000 people with the requisite cybersecurity skills. "We need to do a lot more to make it clear to people how they get into the profession. And we need to set standards because a lot of people who claim credentials aren't really cyber professionals," the official from DCMS said. A Forum member reported that retaining cyber talent is also a challenge. Several commentators encouraged companies to support educational activities that are aimed at building the next generation of cybersecurity talent. A summary of the ACF discussion on the Cyber Talent Shortage can be found here.

In summing up the conversation a subject-matter expert said: "Cybersecurity is clearly now a board level topic but one that board members think is owned by technology. Some of these new cyber regulations cut across every aspect of most businesses, and regulations are helping drive activity at the board level. Improving the regulator's ability to enforce effective regulations is critical because by not doing that we are missing an opportunity to improve standards and performance."

CONTACT

Giovanni Cozzolino
Accenture UK Security Lead
LinkedIn

Kris Burkhardt
Accenture Chief Information Security Officer
Accenture Cybersecurity Forum Chair
LinkedIn

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 699,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.

View the entire suite of ACF roundtable summaries on our webpage – here.