Over the coming years organisations will experience growing disruption as threats from the digital world have an impact on the physical. Invasive technologies will be adopted across both industry and consumer markets, creating an increasingly turbulent and unpredictable security environment. The requirement for a flexible approach to security and increased resilience will be crucial as a hybrid threat environment emerges.

The impact of threats will be felt on an unprecedented scale as aging and neglected infrastructure is attacked and disrupted due to vulnerabilities in the underlying technology. Mismanagement of connected assets will provide attackers with opportunities to exploit organisations.

A recent study from the Economist Intelligence Unit (EIU) found that the speed of technological disruption is making it difficult for regulators to keep pace, and there is a need for more, sensible regulation of technology to safeguard innovation and the benefits of today’s connected society.

However, new regulations will not be able to keep up and fully address the new challenges posed by exponentially advancing technology and its impact on society. Despite early attempts to pass meaningful regulation, the IoT will grow beyond the ability of any government to secure it. A lack of international regulations will be a wide cause for concern, with new and conflicting regulations causing strategic headaches for many organisations: laws designed to protect individual privacy will clash with those designed to make data processing more transparent. Identifying who holds accountability and liability for security will become less clear.

The arrival of 5G, with significantly faster speeds, increased capacity and lower latency, will change existing operating environments. However, these benefits will come at the expense of an exponential growth of attack surfaces. The 5G-enabled devices and networks that underpin society will be compromised by new and traditional attacks, causing chaos and plunging business into disarray.

Critical national infrastructure (CNI), IoT manufacturers, businesses and citizens will all be heavily or totally dependent on 5G to operate. From nation states aiming to cripple CNI – to hackers spying on private networks – 5G technologies and infrastructure will become a key target.

Highly sophisticated and extended supply chains, including cloud technology, present new risks to corporate data as it is necessarily shared with third party providers. IoT devices are often part of a wider implementation that is key to the overall functionality. Since so much of our critical data is now held in the cloud, this opens an opportunity for cyber criminals and nation states to sabotage the cloud, aiming to disrupt economies and take down critical infrastructure through physical attacks and operating vulnerabilities across the supply chain.

In the face of these mounting global threats, organisations must make methodical and extensive commitments to ensure that practical plans are in place to adapt to major technological changes. Employees at all levels of the organisation will need to be involved, from board members to managers in non-technical roles.

Moving forward, enterprise risk management must be extended to create risk resilience, built on a foundation of preparedness, that evaluates the threat vectors from a position of business acceptability and risk profiling.

Enlightened organisations have now moved to a risk-based approach to managing cyber risk. Why? Essentially because the dangers to an organisation from cyber threats have increased in frequency and severity; more organisations are understanding that cyber is entirely embedded across the business and so a cyber threat is actually a threat to business as opposed to something that can be managed from an IT department. This has resulted in a reality check for many.
Organisations of all sizes will need to make sure they are fully prepared to deal with attacks on their valuable data and reputations. The faster you can respond to these problems, the better your outcomes will be.

Driven by demands for increased speed, automation and efficiency, organisations are facing a period of significant technological upheaval as they transition into a hyper-connected digital world. Supporting this world are new, innovative technologies and business models that will create an illusion of stability, reliability and security. However, new and re-energised threats will compromise success and shatter that illusion.

As the world’s businesses, governments, and economies grow more interdependent, knowing how to build resilient organisations and nimble incident response will be vital to more than cyber security. We no longer hide behind impenetrable walls. We operate as part of an interconnected whole. The strength to absorb the blows and forge ahead is essential to competitive advantage and growth, in cyberspace and beyond.

If government departments, regulators, senior business leaders and security professionals do not show a sense of urgency in adopting a realistic, broad-based, collaborative approach to cyber-security and resilience, they will not be equipped to respond quickly and appropriately to the escalating digital and physical collision of cyber-threats.

Above all, organisations rely on trust – and in the digital world, innovative technologies can be misused to erode that trust and digitally naive employees can be exploited, endangering the relationships between organisations and their key stakeholders. Attackers will be presented with the tools and opportunities to ruthlessly target and exploit those who are unprepared. When digital and physical worlds collide, only organisations that take decisive action will prosper.

About the Author

Steve Durbin is Managing Director of the Information Security Forum (ISF). Formerly at Ernst & Young, Steve has been involved with IPOs, mergers and acquisitions of fast-growth companies across Europe and the USA. Having previously been senior vice president at Gartner, he has advised a number of NASDAQ and NYSE listed global technology companies.