The wide-ranging business impacts and risks of cyber attacks

It is only a matter of time before a business will suffer a cyber attack. The potential impact of cybercrime requires that cybersecurity is viewed as a business risk, rather than merely an IT risk. Fundamentally, an organization’s realization is that one as a cyber attack may impact business operations, finance, integrity, and legal exposure to its customers and partners.

In addition, cyber risk has been increasingly linked to data protection and privacy regulatory compliance around the world. For example, the EU’s General Data Protection Regulation (GDPR) that went into effect in May 2018 requires that supervisory authorities be notified, under certain circumstances, within 72 hours of personal data breach. The EU Network and Information Security Directive incident notification requirements for digital service providers (DSP) dictate that DSPs notify the competent authorities within 72 hours of any incident having a substantial impact on the provision of a service. China’s Cybersecurity Law became the first national-level law that addresses cybersecurity and data privacy protection in November 2017. The United States has had a substantial impact on the provision of a service. China’s Cybersecurity Law became the first national-level law that addresses cybersecurity and data privacy protection in November 2017. The United States has having a substantial impact on the provision of a service. China’s Cybersecurity Law became the first national-level law that addresses cybersecurity and data privacy protection in November 2017. The United States has having a substantial impact on the provision of a service.

In order to adequately address the risks from large and complex cybercrimes that are threat, organizations should develop a strong, comprehensive framework that is part of the enterprise risk management and crisis management strategies.

“Who would once have considered large-scale cyber attacks are now becoming normal.”

The Global Risks Report 2018

The World Economic Forum
As part of their extensive crisis management program, we help organizations design and conduct situational training by testing incident response plans and simulating various types of cyberattacks, data loss, and other threats. We provide assurance, regulatory compliance and infrastructure health.

Our team helps organizations establish an investigation framework and governing processes to support the investigation. Forensic response is a significant part of this organization and is to be adequately resourced and funded. We conduct investigations with efficiency and accuracy. In-depth data and evidence collection and preservation in coordination with regulations and laws, and minimal interruption to business operations.

We also work with organizations to form recovery plans that include containment and eradication, and leverage the broader business continuity plan. We take into account short-term measures to secure high-priority environments, restrict access and introduce barriers, while keeping our clients alert to any ongoing threat. Our analysis strategy to reduce the risk of similar attacks happening again.

Cyber response planning

As part of their extensive crisis management program, we help organizations design and conduct situational training by testing incident response plans and simulating various types of cyberattacks, data loss, and other threats. We provide assurance, regulatory compliance and infrastructure health.

Our team helps organizations establish an investigation framework and governing processes to support the investigation. Forensic response is a significant part of this organization and is to be adequately resourced and funded. We conduct investigations with efficiency and accuracy. In-depth data and evidence collection and preservation in coordination with regulations and laws, and minimal interruption to business operations.

We also work with organizations to form recovery plans that include containment and eradication, and leverage the broader business continuity plan. We take into account short-term measures to secure high-priority environments, restrict access and introduce barriers, while keeping our clients alert to any ongoing threat. Our analysis strategy to reduce the risk of similar attacks happening again.

24/7/365 rapid response

Through managed services or preferential provider arrangements, we forge long-term relationships with our clients that enable us to gain deep knowledge of their IT and data environments so we can offer the speed and confidence they need to respond to cyber threats, regardless of the location of their attack.

With our global network, we have teams around the world who work together to forge a 24/7/365 incident intake process so we can respond to a cyber attack at any time of the day.

Secure global infrastructure and consistent global methodology

With numerous advanced security centers, forensic data and data centers worldwide, all of which come with multiple layers of controls, we offer the organizations the connectivity, scale and agility they need to respond to cyber attacks and to manage their data protection strategies.

Governed by a globally consistent methodology, we offer integrated services from one stage of the response life cycle to the next, including comprehensive data recovery and disruption to business operations.

Multidisciplinary team

Our team includes cybersecurity professionals, investigators, data privacy professionals, digital forensics specialists, eDiscovery professionals, forensic accountants, government contract analysts, economists and certified fraud examiners, as well as former ethics and compliance officers, former government auditors, and former prosecutors and regulators.