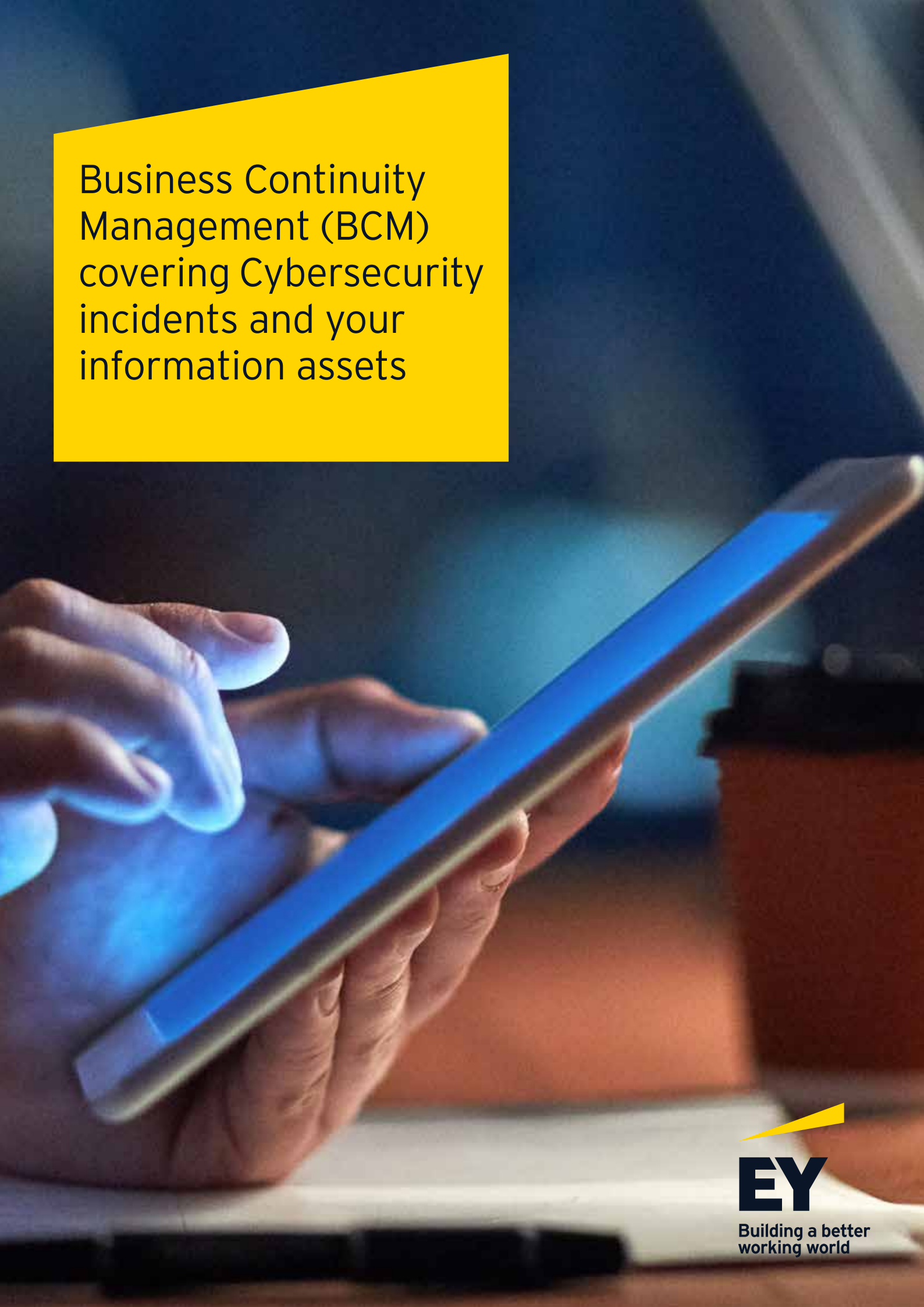
Business Continuity Management (BCM) covering Cybersecurity incidents and your information assets



EY
Building a better working world

Executive summary

In 2019, thanks to the mass commercialization of computing, network communications and IT systems – information technology has quietly solidified itself as a mainstay operation of an organization. Therefore, cybersecurity concerns have shifted toward mitigating operational disruptions and the potential reputational ramifications that might follow.

For any organization, business continuity management (BCM) therefore must be extended to consider the dimensions of cybersecurity. Within the field of cybersecurity, BCM is said to be cornerstone of any cybersecurity effort. However, there is no one-size-fits-all approach to BCM as it inherently depends on the specific context of the given organization. Even from the perspective of cybersecurity, BCM practitioners must consider the technological aspects alongside human processes on equal footing.

Likewise, BCM will be an evolving effort, where it will evolve alongside the changing IT environment and business processes of the organization. The EY BCM framework meets these requirements by fulfilling five stages, namely understanding the business, conducting a business impact analysis and risk assessment, developing BCM policies and procedures, developing business continuity roll-out strategy and help implementing the defined strategy, and performing exercises and conduct awareness training.

Ultimately, by deploying an appropriate BCM program, an organization can maintain an appropriate level of service following an incident that disrupts its information assets. Likewise, an appropriate BCM program will be a step toward aligning the risk exposure of the firm in the path toward greater digitization, integration of information technologies and corresponding complementary business processes.

Adam Sandenholt
Executive Director
Cybersecurity Team
EY Denmark

Introduction

Toward Industry 4.0

The first industrial revolution (Industry 1.0) began at the end of the 18th century, giving the world an unprecedented prosperity through mechanization enabled by water and steam power. The second industrial revolution (Industry 2.0), at the beginning of the 20th century, brought innovations such as mass production using electrified assembly lines. The third revolution (Industry 3.0) was triggered by the commercialization of programmable logic in the early 1970s, bringing computerized machinery and automation on a vast scale.

Industry 4.0 is a rapidly emerging concept seeking to merge the physical and virtual worlds (i.e., internet of things (IoT)). Compared to previous waves of industrial revolutions, Industry 4.0 is challenged by its own vast complexity. Industry 4.0 is largely characterized by vertical networking of production systems, horizontal integration via global value chains, value chain through engineering and an exponential acceleration through technologies.

While most organizations are staying competitive by interweaving the concepts of Industry 3.0 and Industry 4.0, they must also rethink the cybersecurity program and contigency planning to include such topics. This is likewise observed in the C-level executives of Fortune 500 firms, who identify cybersecurity as among the largest contemporary challenges that they face.

With the increased reliance on technologies, such as supervisory control and data acquisition (SCADA), programmable logic controllers (PLC), coordinational systems and network interfaces, firms must reimagine their business continuity management (BMC) planning to encompass the cybersecurity aspect.

Theme of the month: BCM in a digitized economy

With IT systems and technological platforms swiftly becoming the backbone of most organizations, cybersecurity has risen to be among the top priorities in many firms. According to EY Global Capital Confidence Barometer, the greatest fear related to cybersecurity is reputational damage and operation disruptions.[1] Evidently, firms often never recover from a reputational damage following incidents such as a catastrophic data breaches. Equally, operational disruptions can cause major financial damage in the short term. In the long term, downstream business or end customers will lose confidence in the firm as a reliable business partner, causing the abovementioned reputational damage.

Due to increased sophistication of cyber attacks or increasingly systematized cyber crime organizations, firms will be hit by cyber attacks. The increasingly sophisticated nature of cyber crime makes it impossible for any organization to completely safeguard itself against its impacts. Consequently, it becomes imperative for any business to consider cybersecurity in its business contingency plans. As a result, the report for this month will focus on BCM from a cybersecurity perspective. BCM is the notion of facilitating systems to prevent incidents and plan for recovery from any outages. With an appropriate BCM planning, a firm can continue its acceptable level of service and operations while performing a disaster recovery.

The threat of cyber attacks and cyber crime are much more evident in mid-market firms, with the reasons being twofold. First, they tend to contain insufficient defenses due to their smaller cybersecurity budget compared to major, blue chip firms. Second, the cost in effort of conducting cyber attacks or cyber crime has fallen dramatically due to the commercialization of most technologies that enables cyber crime. Likewise, the continued wave of digitization also implies that the IT systems, technological platforms or information assets are more attractive to attack than ever.

The impact is likewise much greater for such mid-market firms. Their inherently smaller size means that operational disruption will lead to irrevocable reputational damage, whereby their customers might cancel existing contracts or even blacklist them. In a worst-case scenario, an operational disruption can trigger a constellation of events that can ultimately gamble the future survival of a firm.

Similarly, contemporary firms are constantly on the vector of change. Within the past few years, EY teams have experienced a substantial increase in M&A activity. This also has an impact on the BCM program of the firms, as they must adjust the BCM plan accordingly to take the coupling of the multiple systems into consideration.

Nevertheless, for organizations of any size, a lackluster BCM program can cause small incidents to snowball into major events that can threaten the survival of the firm. This means that a firm must employ appropriate measures to safeguard itself from eventualities, while striking a balance between business continuity efforts and operations.

For instance, using multisource for key input materials for key processes, a firm can safeguard itself against an outage at single supplier. However, such efforts can also hinder the firm in achieving quantitative rebates from a large purchasing order from a single vendor. Likewise, using multisource can also lead to a firm losing economics of scale from transporting greater quantities of goods from a single supplier. Therefore, an appropriate BCM will fall under the age-old business consideration of cost versus benefit.

[1] *Global Capital Confidence Barometer: M&A – response or resilience,* EYGM Limited, 2019.

Within cybersecurity, the National Institute for Science and Technology (NIST) Cybersecurity Framework has gained significant importance within the immediate past. The NIST Cybersecurity Framework intents to be a security guideline for how American organizations can effectively prevent, detect and respond to cyber attacks – much in line with the traditional cybersecurity preventive, detective and corrective efforts. However, one must not regard BCM merely in the context of cyber attacks, as events that might trigger BCM processes often involve unintended accidents, political events or natural disasters.

Consequently, within the NIST Cybersecurity Framework, BCM falls firmly within detect, respond and recover. An effective BCM program will be able to detect incidents that will trigger business continuity processes. Such business continuity processes will follow a carefully planned process to respond to the incident and recover in such a manner that minimizes the impact of the incident. Continuing in the terminologies of the NIST Cybersecurity Framework, the maturity levels of the framework can also be applied to the application of BCM.

- Tier 1: Partial – It is performed in an adhoc manner, where efforts are identified and performed as reactively. There is limited awareness of risk management throughout the organization.
- Tier 2: Risk-informed – There are organizational-wide policies for risk management, including BCM. In this stage, the management of the organization handles risks as they occur.
- Tier 3: Repeatable – Organizational risk management processes have been formalized and articulated by a security policy.
- Tier 4: Adaptive – The organization is capable of continuously adapting itself based on daily experiences. The organization is driven by analytics to provide insights and best-practices.

Within the International Standards Organization (ISO), BCM is defined in ISO 22301, aptly named "Business Continuity Management Systems – Requirements." Following the industry standards for a BCM program can prove to be a differentiating factor for a firm, as third-party firms will be able to invoke a business relationship with the firm with greater assurance.

[2] ISO 22301:2019: Security and resilience – Business continuity management systems – Requirements," ISO, www.iso.org/standard/75106.html, accessed 01/12/2019

Case on Sony and Mærsk

Case on Sony PS2 in 2004

Sony launched its video game console PlayStation 2 (PS2) in late 2004. Immediately, the newly launched console stroke up a great demand in time for the holiday season of 2004. Consequently, Sony's Chinese production lines were working flat out to fulfill the orders of the world. Sony's primary way of transporting the newly assembled consoles to European customers is via the world's sea lanes – being the preferred transportation method for ferrying massive amount of goods across continents.

However, the shipping route from Asia to Europe almost certainly takes any ship across to Suez Canal. Unfortunately, the shipment bound for Britain became stuck in the Suez Canal when an oil tanker ran aground, halting all traffic in the Suez Canal. This supply issue meant a catastrophic stockout in many of Britain's stores for the PS2 during the vital Christmas season.

As a business continuity measure, Sony hired the Russian-made AN-24 cargo aircrafts to airlift PS2s directly from the ports of China to Britain. This saved the vital holiday sales of the season for Sony, Britain's toy stores and the Christmas shopping of countless families.[3]

Naturally, for Sony, events such as these could have had great business impacts. A lackluster PS2 sales during Christmas would have led to drastic dip in sales of complementary products, such as PS2 games, controllers and accessories. A lackluster PS2 sales could have meant a big failure in PS2's success in Britain. Nevertheless, Sony's BCM efforts minimized the disruptive events in the Suez Canal.

Case on Mærsk in 2017

Taking the focus back to the cybersecurity aspect of BCM, another case occurred at the Danish shipping giant, Mærsk. Mærsk is a logistics firm with an IT setup clustered for high availability, where each Mærsk office has a mirrored setup to all other offices. This does indeed make for excellent availability, as service outage or disruption at a given office location seamless IT support from another office. However, when the NotPetya cyber attack hit Mærsk, the mirrored setup ensured that the cyber attack impacted all connected Mærsk locations, causing a global outage of Mærsk IT systems' coordination among firm's 800 maritime vessels. Just like that, one-fifth of the world's shipping capacity went offline.

NotPetya rode atop EternalBlue, a network and systems penetration tool created by the United States' National Security Agency that leaked in early 2017. EternalBlue is built to take advantage of a Windows protocol and thus allow any party to run software on any unpatched machines. Mærsk's machines were among the unpatched machines – and Mærsk's IT setup allowed NotPetya to spread rampant. Consequently, the entire communications underpinning for Mærsk's logistics infrastructure

[3]Merry Christmas, your PlayStation 2 is stuck in Suez," *The Times*, www.thetimes.co.uk/article/merry-christmas-your-playstation-2-is-stuck-in-suez-5l8j7g2wrtm, 9 December 2004.

was crippled by a destroyed domain controller. The immediate effects were severe — trucks were backing up in long lines at ports, perishable goods were left to rot in containers and the firm faced an unprecedented loss of reputation. Undeniably, the attack on the IT systems of the organization led to a complete meltdown of most of its operations across the world. At the Mærsk procurement, staff were left without options. To meet the needs of customers, staff had to take in shipment orders by personal emails, WhatsApp messages, text messages or any other ways of communication.

In the following days, a desperate search was conducted by despairing IT administrators throughout all Mærsk offices around the world. The administrators finally found a working copy of the domain controller. By pure luck, a blackout in Ghana had a single Ghanian server offline, whereby Mærsk could initiate the slow process of restoring an instance of the domain controller.[4]

Ultimately, with more than US$300 million worth damages, Mærsk was among the hardest hit victims of NotPetya. Within the NIST maturity levels, this is purely in tier 1 partial, where the BCM efforts of the organization are performed reactively as needed. This will inherently lead to much greater time of outage and time for recovery. In the case of Mærsk — the organization might not have recovered without the Ghanian blackout. It is conceivable that Mærsk would have suffered significantly less damage if it had a higher level of BCM preparation and thus a higher NIST maturity level.

Nevertheless, from a BCM perspective, the incident at Mærsk in 2017 showcased the importance of an appropriate implementation and operation of BCM strategy, policy and capabilities. Mærsk was hit from a cyber attack, causing critical operational disruption. This operational disruption then quickly snowballed into a constellation of events which ultimately cost the firm dearly from a financial and reputational perspective.

[4]The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, 22 August 2008.

EY BCM frameworks

EY BCM framework has successfully supported an effective implementation and operation of BCM in areas ranging from the pharmaceutical sector, the financial sector and the public sector among others. The framework focuses on executing five stages, namely

- Understanding the business
- Conducting a business impact analysis and risk assessment,
- Developing BCM policies and procedures,
- Developing business continuity roll-out strategy and help implementing the defined strategy and
- Performing exercises and conduct awareness training.

Understanding the business

A BCM process is highly contextual and thus specific to an organization. Therefore, it is vital to understand the business processes, value chains and dependencies. In this stage, one will also understand the definition of business as usual (BAU).

Business impact analysis and risk assessment

A business impact analysis (BIA) will assist in identifying critical service thresholds, including recovery time objectives (RTO), recovery point objectives (RPO) and maximum time to recovery (MTR). RTO can be considered as the target time defined where a given asset needs to ensure BAU. RPO can be considered as the point whereby the business wants to resume operations from.

Develop BCM policies and procedures

Once the service thresholds have been defined based on a business impact analysis and risk assessment, appropriate BCM policies and procedures can be initiated. In this stage, one will operationalize the high-level strategy into lower-level process descriptions.

The BCM policy will define the daily operation of the BCM, where assets might be backed up in another location to enable the firm to continue limited operations while the firm invokes its recovery planning.

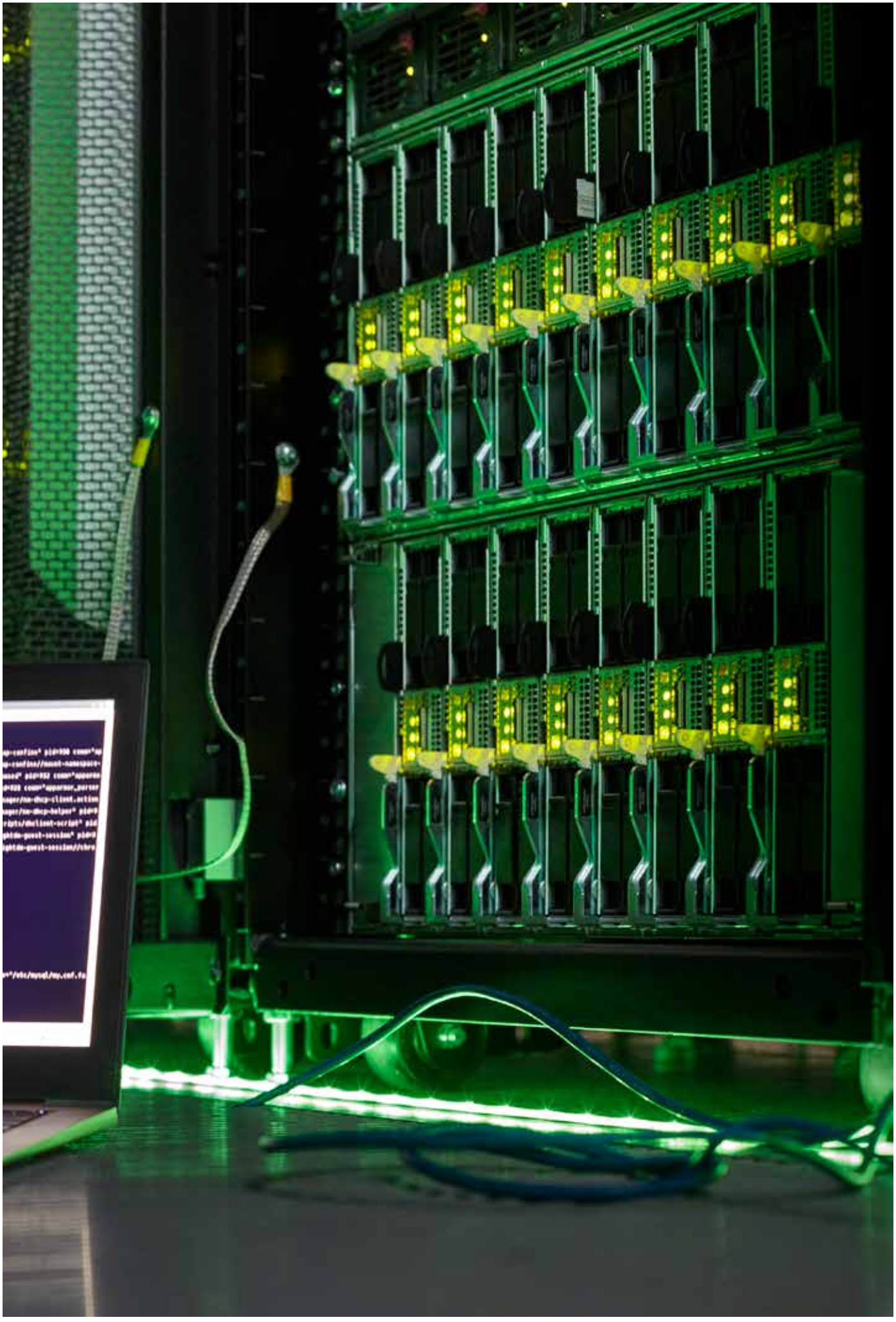
Develop business continuity roll-out strategy and help implementing the defined strategy

Once the goal and strategy have been defined, an efficient implementation assistance is necessary in operationalizing the articulated plans. During the implementation phase, it is vital to involve the appropriate future BCM process owners to engage in the develpopemnet of the plan.

Perform exercises and conduct awareness training

A tabletop exercise is conducted, followed by a full-scale exercise, if required, to test the operational plausibility of the BCM program. General awareness training can be performed to nurture future bottom-up initiatives to improve the BCM program while also facilitating employer buy-in to the BCM program. By performing this additional step, an organization can achieve highest maturity level in NIST, as this allows the organization to continuously adapt itself based on daily experiences.

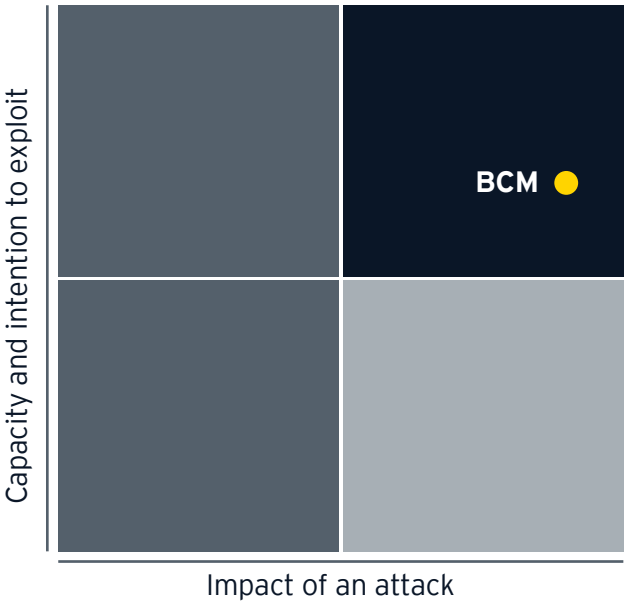
Within the scope of BCM and cybersecurity — one must not consider BCM purely from a technological perspective. Instead, BCM must be considered to encompass much more — from people, processes, systems, infrastructure among many others. Nevertheless, utilizing EY BCM frameworks in any given organization will inherently be subject to the context of the given organization.



State of BCM as of early 2020

The globalization of the contemporary world economy has led to an increasingly integrated supply chains, complex chain of dependencies and a universally dispersed workforce. This trend enables new ways of value creation that has led to ever greater quantities of wealth; however, in protecting the assets, processes and value of the firm, executive management must also consider implementing a BCM program to ensure a swift recovery during adverse events.

EY teams also identifies the theme in the context of our "heat map", based on our hands-on industry experience, which contains two dimensions – the impact of an attack and the likelihood of an exploit. BCM scores very highly in the axis of "impact of an attack," as a lack of BCM can cause incidents to paralyze the operation of the firm. BCM scores high on the axis "capacity and intention to exploit," as firms do experience confidentiality and integrity breaches when following inadequate disaster recovery procedures.



EY severity categories	
Level 1: Minor	This category stands for a very low likelihood of exploit or impact of a potential attack. There is not any recognized capacity of intention to use the probable threat as an attack vector.
Level 2: Moderate	This category refers to general threats with corresponding capacity and intention to cause harm to the firm or organization. Executive management needs to consider this topic in their cybersecurity effort.
Level 3: Severe	This category constitutes a recognized threat, with both considerable capacity and intention to cause significant harm to the organization.
Level 4: Critical	Firms and organizations must pay great care to the threat. This level is reserved for threats that form the cornerstones for any cybersecurity effort.

In addition, EY teams scores each theme on a scale of risk which categorizes them as either minor, moderate, severe, or critical. BCM will inherently safeguard the survival of the firm during an incident. Therefore, based on past events, EY teams can categorize this theme in the category of severe, as inadequate BCM can rapidly escalate events into calamitous outcome.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. For more information about our organization, please visit ey.com.

ED None

ey.com

Authors and contacts

Claus Thaudahl Hansen
Partner
Cybersecurity team
Tel: +45 2529 3639
Email: claus.t.hansen@dk.ey.com
EY Denmark

Adam Sandenholt
Executive Director
Cybersecurity team
Tel: +45 2529 3379
Email: adam.sandenholt@dk.ey.com
EY Denmark

Jonathan Kwok
Advisory Services
Cybersecurity team
Tel: +45 2529 4287
Email: jonathan.kwok@dk.ey.com
EY Denmark