Is cybersecurity the key to your business recovery?

by Tom Clary

Executive summary

Most companies have business-continuity plans in place to help them prepare for and overcome a crisis. But as we are learning in the dawn of the Digital Age, when everything is connected, not making cybersecurity a critical, integral part of such planning — from the outset! — jeopardizes the company's ability to respond to rapidly changing business dynamics. This is particularly true when a global crisis wreaks havoc on communities, supply chains, and entire industries and economies. Applying lessons learned from the COVID-19 pandemic, this paper explains why it's never too soon to begin looking at key cybersecurity considerations. What are your risks? And what can you do about them?

Introduction

In the first quarter of 2020, the globe faced a genuine crisis in the form of the COVID-19 virus. For many companies, the first step in dealing with the threat of the pandemic was to ensure the immediate health and safety of employees and stakeholders.

However, according to a survey of 300 global[1] companies in February 2020, 51% lacked a codified Business Continuity Plan (BCP) to deal with how to maintain operations safely and effectively during the crisis. But even for companies that did have a BCP in place, the scramble to reallocate resources and make quick, large-scale changes to their operations left them exposed to mounting risks if cybersecurity had not already been incorporated.

The rapid spread of the virus forced organizational change and created logistical challenges in nearly every sector of the global economy. Businesses were forced to manage certain operations remotely; millions of employees moved from working on-site to working from home or other remote locations; and according to a survey done by Fortune[2] in March 2020, 94% of Fortune 1000 companies saw disruptions to their supply chains.

The immediate threat to health and safety meant that these sometimes-radical changes to everyday life had to be undertaken rapidly. Even for the most prepared companies, the reality of the COVID-19 pandemic left certain parts of their operations exposed, and left their cyber adversaries licking their lips.

Systemic vs. unsystemic risks

When companies create risk mitigation and Business Continuity Plans, they tend to deal with what they perceive to be high-probability events, i.e., disruptive events that are most likely to occur and can be planned for.

A cyberattack is classified as an unsystemic risk. This means the attack is affecting only one company, or even part of one company, and can be mitigated accordingly. Similarly, an attack to a supplier, vendor, or other third party would also only affect a narrow slice of the overall market. The threat of such specific cyberattacks is already top of mind for risk professionals within most companies.

But their work isn't done because that is only one part of the story. Business Continuity Plans also need to consider systemic risks, i.e., risks and events that can disrupt entire industries or, in extreme cases, the global market. These risks can include natural disasters like earthquakes, hurricanes, and floods, as well as geopolitical conflict, financial crises, pandemics, or cyberattacks themselves.

While systemic risks and events are low probability, they affect many other aspects of your business. Therefore, they must be a factor within your Business Continuity Plan. That's because, when they occur, systemic events change the assumptions made in all other risk planning.

Risks are calculated by evaluating the likelihood of an event, multiplied by the severity of

[1] (2020, February 6). gl-2020-mercer-covid-19-global-survey-coronavirus-impact-to-global-market.pdf. Retrieved from https://www.mercer.com/content/dam/mercer/attachments/global/gl-2020-mercer-covid-19-global-survey-coronavirus-impact-to-global-market.pdf

[2] (2020, March 17). Coronavirus & Supply Chains: Building Resilience | Accenture. Retrieved from https://www.accenture.com/us-en/about/company/coronavirus-supply-chain-impact

its consequence. These assumptions are not static; they must be updated as business circumstances change. A thorough BCP must be dynamic enough to adapt to these events as they happen. Your current exposure to cyber-risks can change quickly, as can the consequences your company could face in the event of an attack or other breach.

Because of the shifting nature of risks, even the most thorough BCP is not fixed. It needs to be revisited and updated regularly, often quarterly, as threats change, both in the likelihood of their occurrence and in the effect the risks pose to your business. Business Continuity Plans should also be updated as significant changes are made internally to your organization. Global, regional, and national threats can become more or less likely to occur, while changes to internal systems, equipment, and strategy can also affect the ability of your BCP to keep operations running effectively.

The global financial crisis of 2007-2008 is one example of a systemic crisis: Its effects were not confined to one bank or one country. The event ultimately impacted companies in every region of the world and in practically every industry.

The 2020 COVID-19 pandemic is another example of a massive systemic shock. Pandemics are low-probability events, which means that many companies were not prepared to deal with the myriad issues the virus caused.

Crises: likelihoods and interconnections

According to a global survey of crisis management, resilience management, emergency management, and business continuity teams (sometimes referred to as resilience departments) across all business sectors published in December 2019 by the Disaster Recovery Institute[3], pandemics ranked as only the 12th most significant issue facing businesses in 2020. This means leading experts predicted a pandemic was less likely to occur than random acts of violence and other low-probability events.

However, those same experts ranked major cyberattacks, severe data breaches, and IT outages as the three most significant issues. Planning to mitigate cybersecurity issues was clearly top-of-mind before 2020, but how many considered the effects another crisis might have on those plans? Can existing Business Continuity Plans withstand geopolitical, climate, health, or another severe crisis?

Cyberattacks have been on the rise since the beginning of the pandemic. At first, common attacks like phishing and malware campaigns were adapted to take advantage of the rapidly increasing anxiety and interest in COVID-19-related subjects. While COVID-19-themed misinformation and phishing attacks quickly leveled off as the public became better informed of the realities of the virus, the rate of overall attacks did not ebb as the virus persisted. According to Microsoft[4], cybercriminal activity was up 20% in June 2020 compared to February of the same year, when the virus really began to take hold.

Companies that had not adequately included cybersecurity in their disaster-recovery or

[3] (2020, December 27). 5th Annual DRI International Global Risk and Resilience Trends Report. Retrieved from https://drive.drii.org/2019/12/27/download-the-fifth-annual-global-risk-and-resilience-trends-report/#:~:text=Developed%20by%20the%20Future%20Vision,factors%20that%20are%20shaping%20it.&#38;text=And%20be%20on%20the%20lookout,2020%20Predictions%20Report%2C%20coming%20soon!

[4] (2020, June 16). Exploiting a crisis: How cybercriminals behaved during the outbreak - Microsoft Security. Retrieved from https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/

Business Continuity Planning were less prepared to deal with a triple whammy: a pandemic, an increase in attacks related to the pandemic, and a less resilient infrastructure due to a suddenly diffuse workforce.

In fact, a report issued[5] by the company Malwarebytes found that 20% of U.S. companies they surveyed reported a cybersecurity incident that was a direct result of employees shifting to working remotely. The companies that fared well had already considered the cascading effects a pandemic or similar event would cause when workers and operations were suddenly shifted to a remote environment.

Your people

Companies dedicate enormous resources to preempt, confront, respond to, and resolve a crisis. Businesses will enlist nearly every function to support. Manufacturing operations, HR, marketing communications, IT, training and development, procurement, legal — the list is comprehensive. Ensuring the cybersecurity of these vital functions is essential. Those on the frontlines — the teams leading the corporate response — may not be looking at the crisis through the eyes of a would-be attacker.

Consider, for example, the operations workforce. Often, companies will reallocate plant personnel or require them to take on new tasks and responsibilities as part of the response plan.

Therefore, before attempting any reorganization, companies need to consider the types of data and technology they require the reallocated workforce to use. Assigning new or inexperienced workers to different roles requiring the use of unfamiliar technology is always a risk. The risk is amplified when malicious activity is on the rise. During a crisis, it's a dangerous combination that could open the door to attacks.

What's more, during periods of heightened activity, personnel who move into a new work environment, including into a new physical space, are even more vulnerable to threats and attacks.

For example, when personnel who are normally assigned to workstations within the plant suddenly switch to working remotely, they become susceptible to common social engineering tactics and threats — like phishing — they might not otherwise confront. Because they are unfamiliar with the systems, procedures, and security protocols companies expect them to work within, they are easier prey to what others would consider routine attack vectors.

Before instituting new work-from-home policies, reallocating the workforce, or undertaking other measures, companies need to know whether their infrastructure and assets remain safe and secure.

Are there anti-virus and other preventive tools in place? Are mechanisms in place to prevent, identify, and warn of phishing and other attacks, even when employees are on VPN? Employees should be cautioned not to use unsecure personal devices for work activities. Employee devices need to be accessible remotely to be managed and wiped if necessary.

Many companies reduced or furloughed staff during the COVID-19 pandemic. Data

[5] 20 percent of organizations experienced breach due to remote worker, Labs report reveals. (2020, August 20). https://blog.malwarebytes.com/reports/2020/08/20-percent-of-organizations-experienced-breach-due-to-remote-worker-labs-report-reveals/.

[6] (2020, June 16). Exploiting a crisis: How cybercriminals behaved during the outbreak - Microsoft Security. Retrieved from https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/

exfiltration (company data taken by exiting employees) is a common practice that could lead to an accidental or intentional data breach. What are your policies and procedures to mitigate these data risks?

And with massive, sudden increases in unemployment caused by the pandemic combined with workers managing devices at home, the risk of exfiltration grows. A report done by the security firm Tessian[6] found that one-third of U.S. and U.K. employees admitted taking company documents when leaving a job, and that rate doubles when the employees do not leave voluntarily.

Your systems

Training and educating your workforce is an important aspect of cyber-risk mitigation, but the backbone of your operations — your Operational Technology (OT) systems — must also have sufficient security and resilience to handle a remote environment and an influx of remote traffic.

Before a crisis like the COVID-19 pandemic, workers in industrial manufacturing environments would often have direct physical access to systems on-site. The pandemic caused changes that has made on-site access either more difficult or sometimes impossible.

Now, workers need to access those same systems remotely. But where one user may have had access only to a particular device, system, or set of systems, others may have had access to the entire operation. As workers relocate from onsite to remote, it isn’t always possible to provide granular level of access to what could be hundreds of employees. This means that in some cases, blanket access must be granted to employees who otherwise would not or should not have had it.

What’s more, many of these systems, which might not be connected or never should be connected, meaning they are accessible only by workers who are physically present, are now being connected to enable remote access. The result? Of course: They become vulnerable to cyberattack, just like any other IT device or system.

Many of the systems that control the world’s most critical infrastructure are inherently vulnerable. That is because they were designed, engineered, and installed decades ago, when cybersecurity wasn’t even a thing. Industrial control systems and network security often lags IT network security. Now, in the haste to respond to a systemic event, the systems responsible for the most critical operational tasks are not only accessible to more of your workforce, they are more accessible to cybercriminals as well. In other words, while remote access allows these systems to stay up-and-running during a crisis, an attack can cause them shut down just as quickly, and the results can be devastating, even life threatening.

In the industrial manufacturing and critical infrastructure markets, the focus is often on securing the operations, especially on the critical control and safety systems that automate and protect the operating environment. These OT systems often have strong pre-established security processes. During a disaster, it is even more critical to ensure workers follow security processes. Regardless of conditions outside, on the inside of the operations, safety is always the priority.

[6] (2020, May 22). The State of Data Loss Prevention 2020 | Tessian Research. Retrieved from https://www.tessian.com/research/the-state-of-data-loss-prevention-2020/

When it comes to controlling risks to operations and business, most executives discuss efficiency, reliability and productivity. But safety is always the top concern.

A visit to any refinery or other critical infrastructure site will make this fact apparent. When visiting a facility, normally the first thing you will be told and the first subject discussed are the plant's safety policies and procedures. Just as crucial as setting policies is empowering people in these environments to enforce the policies. If they see an unsafe condition, they report or act on it as a matter of course. That is what happens when safety is a fundamental part of the culture.

There is a clear link between safety and cybersecurity. In the context of industrial manufacturing, if a hacker successfully compromises a mission-critical system, the consequences could be drastic. It is not just the risk of financial loss or asset damage. A successful attack could lead to an environmental disaster, severe injuries, and even loss of life.

During a crisis, when operations are more exposed to the risk of cyberattack, safety and cybersecurity need to be on equal footing and shared priorities.

Data privacy

When a crisis hits, disruption to normal working conditions puts a strain on established security protocols and can put employees in unfamiliar working situations. Companies with strong security software and encryption, and physically secured devices, are still vulnerable to attack through their employees themselves. Even the most state-of-the-art bank vault is only as dependable as the person holding the key.

According to a 2020 report by Verizon, human error is the second-most common cause of data breaches, after criminal hacking[7]. One in five incidents can be attributed to simple mistakes by employees. This doesn’t even factor in the risk of malicious actors taking advantage of employees through phishing, malware, or pretexting. Simply sending the wrong email attachment or sharing passwords to sensitive databases can lead to damaging data breaches.

Effective and consistent employee communication, as well as strengthening your cybersecurity culture, is crucial to preventing careless mistakes that leave businesses exposed to threats. Communication plans around data privacy and cyberthreats should be ongoing, but they must also be a key element of any Business Continuity Plan.

Moving employees to a remote working environment en masse can put a strain on existing security infrastructure. Employees might ship sensitive information from a company-issued, VPN-connected device to a personal device that is connected to a thoroughly insecure home network. Web conferencing or instant messaging services that are not sanctioned by the IT department are more likely to be used for business and non-business activities as employees connect from home. Even the increased use of virtual meetings can leave sensitive information potentially visible to outside parties on secure networks through screen sharing.

[7] (2020, July 7). 2020-data-breach-investigations-report.pdf. Retrieved from https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

A Business Continuity Plan must include steps to ensure that all employees are aware of the risks associated with straying from security protocols. Policies around accepted use of direct messaging applications, video conferencing, file storage, and email must be clear, easy to understand, and communicated often to reduce these vulnerabilities.

Companies need to take a longer-term view and quickly instill a “cyber first” culture. It goes beyond the simple guidelines and best practices. Yes, they need to address the basics:

- Be very cautious of external emails, especially anything attempting to solicit you to click a link.
- Keep OS and all software patched. Accept all software updates from your company IT department promptly.
- Keep work data on your work computer. Don't use personal devices unless secured and approved by your IT department.
- Effectively manage passwords. Avoid using the same password for multiple systems, and ensure passwords are not easy to guess.

But to drive that “cyber first” mentality, they need to make everyone, everywhere, aware of and responsible for cybersecurity, regardless of role and location, and then empower them to act.

More than ever, an educated and aware workforce will be the best protection against cyberattacks that threaten the safety of an operation. In many cases, your people are the first and last lines of defense. The challenge will be to ensure cybersecurity is an integral part of the operations lifecycle by providing ongoing training; installing best practices and ensure everyone always follows them; then performing regular risk and threat assessments to identify and fill gaps, including gaps in your employee skill sets.

Supply chain

There are myriad risks to consider in every step of your supply chain when developing a Business Continuity Plan. But with systemic incidents that affect an entire industry — or in the case of COVID-19, the entire global economy — the risks are compounded.

When operations are disrupted by some exogenous event, your organization’s cybersecurity risks will increase. But when each interconnected node in your supply chain — from partner, supplier, third-party vendor, customer — are equally affected at once, the risks become nearly impossible to quantify.

How will your business function if one of your critical suppliers falls victim to a cyber incident amid the chaos caused by a pandemic? How can you ensure that your customers’ network is safe and reliable enough to accommodate remote testing, installation, and maintenance?

A cyber incident at one of your suppliers, or your supplier’s supplier, could not only expose your company and customers to potential vulnerabilities, but can add unanticipated delays and bottlenecks, as well as establishing new chokepoints in a complex and interconnected supply network.

Having contingency plans in place to deal with potentially compromised suppliers or downstream distributors or resellers is key to maintaining business continuity in a crisis.

Partners and third parties

Most organizations are increasingly relying on third parties not just in their supply chain, but in support services, technology partners, consultants, vendors, and contractors. As companies focus more on core competencies and increase outsourcing to curb costs and increase efficiency, they are opening even more potential doors to cyberattack through others.

Consider this example. In 2013, the U.S. retail giant Target was famously the target of a data breach exposing potentially millions of consumer credit information to be compromised. The attackers did not strike Target directly. Rather, they infiltrated one of the company's HVAC vendors through a phishing attack. After compromising the vendor through malware, attackers gained access into Target's internal system and were able to pilfer the consumer data.

A business the size of Target deals with potentially thousands of third parties, each bringing a unique set of risks to business operations, data privacy, and reputation. An HVAC vendor may have been low on the list of potential third-party marks for cyberattack (a very low-probability unsystemic risk). Yet despite the high-profile nature of this breach occurring more than seven years ago, according to a 2020 report by Deloitte[8], only 15% of organizations globally integrate third-party risk management into their overall risk management programs.

Incidents like the data breach at Target have only increased over the past decade, and systemic risks only add to the inherent threat of third-party relationships. This means that nearly every facet of an organization is at risk of allowing an attack to a third-party to affect the organization.

Risk management for third parties cannot just be the domain of supply chain or IT departments. Third-party vetting and security need to be part of a focused, enterprise-wide commitment to cybersecurity standards, audits, and compliance with all third parties across functions, business units, and countries.

When choosing partners, vendors, suppliers, and parts of the supply chain, companies must have a plan in place to ensure that its partners are not adding to the list of cybersecurity threats they're already facing. This includes an assessment of the third party to ensure that their level of security is up to the same standards that each company applies to themselves.

All the best practices your company implements to secure your network and devices can be negated when vulnerabilities are not addressed by your connected third parties. These assessments should not be limited strictly to business continuity planning but applied more broadly as an overall business plan.

Just as your company is more vulnerable to attack during a crisis, the same is true of your third parties. That's why a traditional cybersecurity assessment of partners is not necessarily enough. You must also be aware of their contingency plans in the event of a crisis. Under normal conditions, you may have a third-party that meets all your own security standards and protocols. But in a crisis, their existing procedures are likely to be affected. How do they plan to maintain a culture of security, as well as keep their own data safe from attackers who could use third parties to infiltrate your company?

[8] (2020, August 7). Third-Party Risk Management (TPRM) Global Survey 2020 | Deloitte US. Retrieved from https://www2.deloitte.com/us/en/pages/risk/articles/third-party-risk.html

What can you do now?

Your Business Continuity Plan is designed to keep production running while satisfying orders and servicing your customers during a disaster or crisis. Your most critical business functions must continue to operate, but conducting business from a recovery posture can add to your risk of attack. It can be difficult to do anything that might further slow your recovery or response to a crisis, but an oversight at this moment is the precise vulnerability cybercriminals are looking to exploit.

There are steps you can take to consider cybersecurity as part of your BCP. Some basic best practices include:

- Collaborating with cross organizational teams, especially your IT and OT security teams, when drafting your BCP. Any step that is taken to ensure critical business activities aren't interrupted should be analyzed through a cybersecurity lens to identify any increase to exposure. If your BCP increases your susceptibility to attack, it either needs to be reconsidered, or additional mitigating steps should be added.
- Consider how potential changes in employee working conditions could add to cybersecurity risks. If you have employees suddenly working remotely, or forced to work from an unfamiliar site, plan for how you can make sure they are connected and productive without compromising critical data or systems.
- Increase employee awareness to the heightened threat of attack. Working outside the office can lead to employees becoming less diligent about practicing appropriate cyber-hygiene. Consistent communication and education are vital to keep cybersecurity top of mind no matter where your employees are working.
- Test your plan to verify that it will work to keep your operations up-and-running. Have you thought of everything? How will moving operations to a secondary site, or allowing for full-time remote working affect lead times, production planning, and inventory needs? Can you confirm your suppliers and customers can adapt during your recovery time during unsystemic crises? Are they equipped to stay operational themselves during systemic events? How are they fortifying their own networks from increased attack opportunities? This is your chance to evaluate your plan for weaknesses and address them before the crisis.

Failing to look at your critical operations holistically, focusing on the cyber-effects of each decision, could undo any positive effects of your BCP. Avoiding downtime or other short-term delays is imperative for most businesses, but for some businesses a cyberattack is an existential threat.

Conclusion

Through the COVID-19 pandemic, we've seen how crises can disrupt business operations on a massive scale. When health and safety are top priorities and contingencies must be put in place immediately, without proper cyber planning, your company has never been at deeper risk.

As we have seen, many companies are still reacting to their business risks, especially the cybersecurity risks that threaten not only their overall business performance, but also impact the health and safety of their people, assets, and operations across their extended ecosystems, including their customers.

It has never been more clear: In order to protect and improve overall business performance and resiliency, companies need to consider how to proactively and continually manage their cyber risks across the enterprise lifecycle as part of a robust risk-management and business continuity strategy.

Cybersecurity risks, especially cyber risks related to systemic events, are dynamic: They change every day. Therefore, the approach to managing these risks needs to be dynamic and ongoing. The best approach to reducing, mitigating, and even eliminating current and future risks is to establish a strong cybersecurity foundation that addresses the dynamics of your people, processes and technology.

But where to begin? The first step is to ensure cybersecurity is at the foundation of your overall risk-management and risk-assessment strategy and matrix. By understanding your risk threshold and appetite, you will be better positioned to develop and implement a holistic strategy that tackles the dynamics of your unique environment.

Many companies simply do not have the talent and resources to take this on themselves. Because the stakes are so high, it is best to find a partner who has the expertise to help you design and implement the program that is right for you. In most cases, you will need monitoring, maintenance, and training services. In addition, you'll need the technical expertise to help integrate your existing technology, even if it is from multiple vendors and of multiple vintages. Take a technology-agnostic approach to devise a flexible solution that fits your specific needs.

The goal is a holistic, dynamic program that will continually identify, assess, and minimize your risks and threats. With the right strategy, coupled with a flexible, scalable solution, you will soon know and be able to visualize where your threats and gaps are. More importantly, you will have the people, processes, and technology in place to reduce the potential impact the next event — be it systemic or unsystemic — has on your business performance.

Cybercriminals are quick to take advantage of global events, exploiting vulnerabilities and gaps wherever they can be found and leaving your company particularly exposed at the worst possible time. Without a strong cyber-influenced Business Continuity Plan, dealing with the effects of one sudden crisis can open the doors to an accompanying and potentially crippling cyberattack, one that could threaten your very business survival.

The next event can strike at any time. The companies that are planning now will be best positioned to endure.

About the author

Tom Clary is the global director of cybersecurity communications for Schneider Electric. He has more than 25 years of industry experience, including more than 10 years of focus on industrial automation and process control, process safety and cybersecurity in the manufacturing, energy, oil & gas, infrastructure management and building management industries. A recognized senior communications strategist and counselor, he has received multiple awards for his work in the fields of crisis and change management, including Schneider Electric's Global Recognition Award for excellence in cybersecurity incident response and crisis resolution.

Schneider Electric's team of experts provide vendor-agnostic solutions that support your needs for cybersecurity protection across all business types and industries. We apply a rigorous mindset, policies, and methodologies in the development of our products and the implementation of our solutions in support of our customers' digital transformation. Visit se.com/cybersecurity to learn more.

Schneider Electric

998-21085205