Launching into Cyber Security September 2020

Home/ / My courses/ / LCYS_PCOM7E September 2020/ / Unit 1/ / Collaborative Learning Discussion 1/ / Initial Post - Cyber Security Today/

« Collaborative Learning Discussion 1

Lewle Seneviratne

Initial Post - Cyber Security Today

56 days ago

7 replies

Last 39 days ago

In an era of digitalization to create exclusive competitive advantage in the business world has moved “risk management thinking” to go beyond traditional risks to have robust measures to safeguard our dependency on digitized solutions and perceiving their vulnerabilities regards to integrity, confidentiality and accessibility.

For example, Denmark being ranked at top three as the most digital country in the European Union (European Union, 2020), in their 2020 threat assessment concludes that cybercrime and cyber-espionage pose high economic and political threat to Denmark and will continue to remain serious with continued digitalization. Moreover, the threat assessment 2020 highlights the fact that new routines underpinned by COVID- 19, have constantly attracted cyber-hackers to exploit current events, developments to their own advantage (Centre for Cyber Security, 2020).

Potential impact of cyber-attacks to some businesses would be risks of losing credibility and brand reputation in their market, while some are more prone to risks related to unreliable data, stolen intellectual property, financial losses due to digital fraud or failure of key operational IT systems. UK’s 2019 Cyber Security Breaches Survey quantified the fact that about 32% of UK businesses had cyber-attacks in 2019 and the average cost to the business was GDP 4,180, while the average costs faced by medium/large enterprises tend to be much higher ranging GDP 9,270 to GDP 22,700 (Department for Digital, Culture, Media and Sport, 2019).

Reference List

Center for Cyber Security. (2020) *The cyber threat against Denmark*. Available from: https://fe-ddis.dk/CFCS/publikationer/Documents/The-cyber-threat-against-Denmark-2020.pdf [Accessed 24 September 2020].

Cybersecurity Ventures. (2019) 2019 *Official Annual Cybercrime Report* Available from: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf [Accessed 23 September 2020].

Department for Digital, Culture, Media & Sport. (2019) *Cyber Security Breaches Survey 2019: Main report* Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875799/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised.pdf [Accessed 25 September 2020].

European Commission. (2020) *The Digital Economy and Society Index (DESI) 2020*. Available from: https://ec.europa.eu/digital-single-market/en/desi [Accessed 24 September 2020].

European Court of Auditors. (2019) *Challenges to effective EU cybersecurity policy.* Available from: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [Accessed 25 September 2020].

375 words

Reply

7 replies

1

Post by Shoumik Chakraborty

Peer Response - Cyber Security Today

54 days ago

Peer Response - Cyber Security Today

As mentioned in the parent article, the CIA being the building block for information security risk assessment, there are other concepts such as AAA or Protection Mechanism contributing to business-driven risk assessment and needs discussion. (Stewart et al., 2015: 4-13).

The CIA facilitates determining asset criticality for risk assessment where "Confidentiality" defines the restriction over data, "Integrity" determines the correctness of data, and "Availability" provisions data-accessibility to authorized personnel (Stewart et al., 2015: 4-7).

Stewart et al. (2015: 8-12) defines security concepts other than CIA and discusses "identification, authentication, authorization, auditing, accountability, and nonrepudiation" as a part of AAA services.

1. Identification defines the identity of the user trying to access data such as username.
2. Authentication defines the verification of the user identity, such as a password or token.

3. Authorization defines access to the data requested by the user, such as admin or read-write, etc.
4. Auditing tracks all the views and changes in the data.
5. Accountability enforces users to accept the consequences of data alteration and accessibility. For example, HR has access to all the employee personal data, but unauthorized access can lead to disciplinary measures according to the company policy.
6. Nonrepudiation ensures the non-deniability of user events and thru other AAA services.

The protection mechanism defines the "Layering" of controls, the "Abstraction" of data structure, "Data Hiding" and "Encryption" (Stewart et al., 2015: 12-13)

The correct categorization of assets & data, periodic gap assessment, implementation of adequate controls, and proper risk treatment plans can minimize the risk for any organization.

References

Stewart, J.M., Chapple, M. & Gibson, D. (2015) CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide. 7th ed. Wiley India Pvt. Ltd.

280 words

Reply

2

Post by Laura Rivella

52 days ago

Peer Response - Cyber Security today

Hi Lewle,

I would like to build on the very good point you made on the 2020 threat assessment.

New routines underpinned by Covid-19 have indeed attracted more hackers, current events have opened more opportunities and shifted priorities for some malicious actors.

Opportunities appear to present themselves at every level.

Covid-19 surveillance systems run by governments through apps have proven themselves to be the security risk that many feared. In India, eight million patients had their personal and medical details compromised after vulnerabilities were discovered within the Surveillance Platform Uttar Pradesh Covid-19. Software bugs were detected in early August, yet the issue was not remediated until September 10. (Muncaster, 2020)

Data exposed included full names, addresses, diagnoses, symptoms, medical records, and phone numbers.

Data on the potential vaccines is also a hot target. (Barnes & Venutolo-Mantovani, 2020) Obtaining vaccine data or spying on its development is deeply tied to the question of nationalism, in addition to being a potential revenue source if such information were to be sold. Rather than cooperate through global mechanisms to develop, manufacture, and distribute a vaccine against the coronavirus, countries with the means to do so have prioritized national access to a vaccine. (Fidler, 2020)

International lawyers have issued statements on international law applicable to cyber operations targeting vaccine research stating that harmful cyber activity may undermine States' and global efforts to contain and recover from the COVID-19 pandemic. (Oxford Institute for Ethics, Law and Armed Conflict, 2020)

It is worth noting however that cyber espionage is not prohibited by international law. (Schmitt, 2017)

It does not appear to be an issue only for pharmaceutical companies, softer targets such as universities are also at risk and hackers have conducted ample digital reconnaissance on the University of North Carolina and other schools doing cutting-edge research. (Fidler, 2020)

Reference list

Barnes, J. E. & Venutolo-Mantovani, M. (September 5, 2020) Race for Coronavirus Vaccine Pits Spy Against Spy. The New York Times. Available from: https://www.nytimes.com/2020/09/05/us/politics/coronavirus-vaccine-espionage.html?referringSource=articleShare [Accessed 29 September 2020].

Fidler, D. P. (September 14, 2020) The Cyber Side of Vaccine Nationalism. The Council on Foreign Relations. Available from: https://www.cfr.org/blog/cyber-side-vaccine-nationalism [Accessed 29 September 2020].

Muncaster, P. (24 September, 2020) Millions Exposed in #COVID19 Surveillance Platform Snafu. Info Security Magazine. Available from: https://www.infosecurity-magazine.com/news/millions-exposed-covid19/ [Accessed 29 September 2020].

Oxford Institute for Ethics, Law and Armed Conflict (2020) The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research. Available from: https://www.elac.ox.ac.uk/article/the-second-oxford-statement [Accessed 29 September 2020].

Schmitt, M. N. (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press.

456 words

Reply

Post by Arun Thomas

Peer Review - Initial Post - Cyber Security Today

49 days ago

The post describes the threats and impacts of cybersecurity and the companies' robust measures to improve cybersecurity.

I agree with the fact that businesses around the world have understood the importance of cybersecurity to stay ahead of the competition. Also, they have improved their strategies to deal with legal risks and the vulnerabilities regarding integrity, confidentiality, and accessibility.

We agree that the rate of cyber attacks in 2020 has been increased and is mainly due to the COVID-19 pandemic. The INTERPOL assessment on cyber attacks shows a significant target shift from small businesses and individuals to major corporations, critical infrastructures, and governments. Not only Denmark, but every country faced economic and political threats due to cyber attacks during 2020.

The losses due to cyber attacks might be different for different businesses, but the fact is that all companies should face some losses in the case of cybersecurity breaches.

Review Summary:

The author researched the impacts and threats of cybersecurity for companies and governments, especially Denmark. The author could have concentrated on his/her vocabulary and punctuations, which might have improved the article's overall readability. The author could have included information on why cybersecurity is a global issue and its legalities.

200 words

Reply

4

Reply to Arun Thomas from Samuel Danso

48 days ago

Re: Peer Review - Initial Post - Cyber Security Today

Very interesting data presented by Lewle. Even though we do expect that with more activities moving online due to Covid-19, we would expect that the security measures including investments and would also increase proportionally.

With Denmark being among the top 3 digital countries in Europe, it would be interesting to see a comparison between Denmark and the UK in terms of rates of cyber-attacks, breaches, impacts, and investments for periods before Covid-19 and possibly during Covid-19.

For example, if 35% of UK businesses had cyber-attacks in 2019, what is the figure in Denmark and what impact did it have on businesses in terms of GDP?

105 words

Reply

5

Post by Amy Lord

Peer Response - Cyber Security Today

43 days ago

Hi Lewle,

I completely agree with everything you're saying, you've clearly thoroughly researched the topic.

The digitalisation of the modern world poses an enormous threat to cyber security. Back in 2018 Cisco estimated that there would be 50 billion online connected devices by 2020 and that most of those would be some form of internet connected smart device, known as the Internet of Things (IoT) (Khan and Salah, 2018). IoT devices have historically been significantly more vulnerable to attacks and have granted attackers easy access into networks they may not have otherwise had access to.

In October 2016, a distributed denial of service attack (DDoS) was carried out on some high profile websites. What made the attack unique was that the compute power for the DDoS was provided by a botnet of previously hacked baby monitors, webcams and other IoT devices (Pultarova, 2016). Had the manufacturers of these products not tried to gain a competitive edge by connecting their devices to the internet, an attack like this would never have been possible.

References:

Khan, M. and Salah, K., (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, [online] 82, pp.395-411. Available at: [Accessed 8 October 2020].

Pultarova, T., (2020). Webcam hack shows vulnerability of connected devices. *Engineering & Technology, IET*, (11), p.10.

217 words

Reply

6

Post by Lewle Seneviratne

Summary Post - Cyber Security Today

39 days ago

From the first three units of the module and peer responses, many important discussion points have been raised in regards to today's cyber-security environment.

Today, cyber-threats facing organisations' systems and data are a far cry from those of the past, and traditional recovery strategies and processes are not enough to keep up with the threats. The Global Risks Landscape 2020 issued by the World Economic Forum, cyberattacks were ranked among the top 10 risks regarding the likelihood and magnitude of the impact.

Though digital evolution and connectivity are crucial for achieving organisational success; as two sides of the same coin being connected also, mean being more vulnerable to security attacks. Once the vulnerability is exploited, it can disrupt confidentiality, integrity, and availability (CIA) of information security. By examining an organisation's overall security posture through the lens of the classic CIA triangle, and then modernising it accordingly, vital for an organisation to stay secure, focus, and resilient when faced with today's rapidly changing cyber-threat landscape (Renneker, Norton, K. & Mehta, 2019).

Authorities, infrastructure providers, businesses, organisations and individuals face distinct challenges related to cyber-risks, as they are highly interconnected globally through perimeter-less networks. Today, technology drives change in cyber-crime behaviours, making them more profitable than drug trade (Cybersecurity Ventures, 2020). As cyber-criminals have continued to adapt and grow in sophistication by year-over-year, cybersecurity spreads from corporate agendas and becomes a household issue (Deloitte, 2018).

In conclusion, as attention increases, the new trend in cyber-risk demands a holistic approach towards cyber-risk management.

i. A high level of individual awareness and competences in cyber-security and data privacy is crucial, as most intrusions are due to human error. Hence, a cyber-security culture within society through education and public-private partnership initiatives can serve as a differentiator.

ii. Building regional/national standards and solutions to monitor traffic and networks; to detect breaches and to have recovery plans to prevent open network breaches. For example, setting nationwide high standards for the sender and receiver identification such as NemID in Denmark (Deloitte, 2018).

iii. The Internet of Things (IoT) with many billions of interconnected objects around the world, is expected to increase to 50 billion by 2020 (Lord, 2020). In such a scenario, any product or service with a lack of cybersecurity measures increases the vulnerability to cyber-attacks. As such, these circumstances demand a robust measure to include cyber-security measures from the beginning of the product design. Public-private partnerships initiatives to set standards that can guide companies on how to include security at the initial stage of product development and post-certification process to assess the reliability can create a greater sense of responsibility.

Reference List

Cybersecurity Ventures. (2020) Cybercrime Damages $6 Trillion By 2021. *Cybercrime Magazine*. Available from: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ [Accessed 10 October 2020]

Deloitte. (2018) *The future market for cybersecurity in Denmark*. Available from: https://innovationsfonden.dk/sites/default/files/2018-07/thefuturemarketforcybersecurityindenmark.pdf [Accessed 3 October 2020].

European Union Agency for Law Enforcement Cooperation. (2020) *Enterprising criminals: Europe's fight against the global networks of financial and economic crime*. Available from: file:///C:/Users/i0357750/Downloads/internet_organised_crime_threat_assessment_iocta_2020.pdf [Accessed 11 October 2020].

Organisation for Economic Co-Operation and Development - OCED. (2017) *OECD Digital Economy Outlook 2017*. Available from: https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generat ed/document/en/9317011e.pdf [Accessed 12 October 2020].

Renneker, P. Norton, K. & Mehta, R. (2019) Using the CIA Triad to Boost Cyber Resilience. *Risk & Compliance Journal*. Available from: https://deloitte.wsj.com/riskandcompliance/2019/05/27/using-the-cia-triad-to-boost-cyber-resilience/ [Accessed 10 October 2020]

World Economic Forum. (2020) *The Global Risks Report 2020*. Available from: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf [Accessed 4 October 2020].

614 words

Reply

7

Reply to Lewle Seneviratne from Fred Vincent 39 days ago

Initial Post: Emerging issues and economic benefits of investing in cyber security

Global issue of Cyber Security

Cyber-security also called as information technology security entails the process of defending and protecting servers, computers, data, networks, mobile devices and electronic systems from malicious attacks (Graham, Howard and Olson, 2016). The UN report highlights of cyber-security as a global issues due to the increased proliferation of information and communication technologies (ICT) between companies located in different countries followed by the series of cyber-attacks and breaching of regulations. Since 2011, the rate of cyber-crime has increased with more than 1 million cybercrime are recorded on a daily basis. Cybercrime has developed as one of the biggest industry which exceeds trillion dollars of revenue encompassing frauds, intellectual property and identity theft (United Nation, 2011). Therefore, in order to control the impact of cyber-security threats, it is essential for companies to create their cyber-security architecture to intertwine functionalities to protect the company's data from hacking and phishing activities. Network security architecture framework needs to be developed to highlight standards, policies, structure and behaviour of computer network to counter and protect the company's data from illegal activities (de Koning, 2017).

Investment in Cyber security

Every business draws more value from its company data; there is a greater cyber-security risk that these companies carry. There has been a $13 trillion worth of data-fueled applications projecting new activity by 2030 (Gibbons, 2020). With frequent cyber-attacks coupled with the weightage of the data-fueled activities, companies must invest in affordable and powerful cyber-security solutions to reserve the business from unprecedented data leaks. One of the primary reasons for investing in cyber-security is to protect the data that fuels the business as through cyber-security solutions, the companies would be able to protect themselves from identity theft or other financial damage. Investing in cyber-security solutions also helps the companies to maintain productivity as the cyber-attacks focus on data and costs that have a significant impact on productivity (Wang, 2017). Therefore, investment in cyber-security solutions would help to safeguard the critical files from going out of actions thereby reinstating productivity.

Economic benefits to the companies

Cyber security issues faced by the companies could be addressed through effective investment into cyber-security solutions. While the cyber-security investments involve costs of expert headcounts, implementation cost, economic risk and training provided to the employees, their economic benefits is paramount to understand the feasibility of the investment on cyber-security solutions (Gontar, 2019). Cyber-attacks cause obvious financial distress for the companies which are an immediate monetary loss for the business. This directly impacts the revenue stream of the business and implies irreparable financial damage. One of the economic benefits of investing in cyber-security solutions is that it would be to insulate the financial architecture of the business and prevent the ransom ware to interfere with the revenue streams of the companies. On the other hand, cyber-security solutions help to safeguard the network within which critical files are stores that are operated by the employees. Securing these critical files would deinstitutionalised the productivity of the company and ensure economic benefits in the form of higher sales and profitability (Lloyd, 2020).

Implication of breach of regulations and laws

In the current business environment, companies despite investing in the development of cyber-security are still facing issues in controlling the prevalence of cyber-security threats resulting in damaging the company’s market image. There are several cyber-security regulations and laws practiced in different countries such as Data Protection Act 1998 in the UK, Privacy Act of 1974 in the US and UN’s International Law on Cyber Security (Adonis, 2020). Intentional or unintentional breach of any of the above-mentioned cyber-security regulation and law by companies has negative implications on businesses such as reputational damage as cyber threats are most likely to impact on the trust level of customers and stakeholders who would face the fear of losing their personal credentials and data to illegal hackers. Companies facing cyber threats regularly are also likely to lose their opportunity to attract best talent, investors and suppliers (Dunn, Erwin and Hadley, 2017). Consequently, the implication of breach of cyber-security laws can also result in lowering the competitiveness level of the business impact of cyber threat is most likely to result in generating a loss of revenue. Security breach negatively impacts businesses to lose a significant amount of money thereby making it difficult for them to compete against its rivals.

The case of Wal-Mart

The growing battle over global cyber-security issues has triggered sophisticated companies to demand personalised customer data.Wal-Mart had violated the California Consumer Privacy Act (CCPA) after compromising with the customer's information and exposing the data to the risks of fraud and identity theft (Muncaster, 2020). In this regards, Wal-Mart had made an investment worth $85 million in Team8, a cyber-security solutions startup company headed by the former leader of the top military intelligence unit of Israel. Through this solution, Wal-Mart has been able to securely share customer data with the vendors in the cloud and also allow the company to use machine learning to acquire customer data relevant to make a better prediction about the needs and wants of the customers (Cheng, 2018).

Approaches to mitigate cyber-security issues

There are various measures that could be applied in business to counter cyber-security threats such as

- Installing and updating virus protection software regularly
- Backing up of data on a regular basis (Hamrick, 2019).
- Offering security training to employees
- Abiding by data security laws and regulations

References

Adonis, A.A. (2020) *International Law on Cyber Security in the Age of Digital Sovereignty*, [Online], Available: https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/ [12 October 2020].

Cheng, A. (2018) *Why Walmart Is Investing In A Startup Founded By Former Leaders Of Israel's Top Intelligence Unit*, [Online], Available: https://www.forbes.com/sites/andriacheng/2018/10/23/why-walmart-is-investing-in-a-startup-founded-by-former-leaders-of-israelis-top-intelligence-unit/#349a4436d737 [12 October 2020].

de Koning, (2017) *The Best Framework for Security Architecture*, [Online], Available: https://www.linkedin.com/pulse/best-framework-security-architecture-pascal-de-koning/ [12 October 2020].

Dunn, M.D., Erwin, M.J. and Hadley, K.M. (2017) *Cybersecurity: Regulatory and Litigation Consequences of a Data Breach*, [Online], Available: https://www.clm.com/publication.cfm?ID=5587 [12 October 2020].

Gibbons, (2020) *Why Investing In Cybersecurity Makes Sense Right Now*, [Online], Available: https://www.forbes.com/sites/serenitygibbons/2020/04/09/why-investing-in-cybersecurity-makes-sense-right-now/#21c5aa013d22 [12 October 2020].

Gontar, L.O. (2019) 'Legal procuring of international information/cyber security of the digital economy: economic and legal aspects', *E-Management*, vol. 2, pp. 61-66.

Graham, , Howard, and Olson, (2016) *Cyber Security Essentials*, 1st edition, New York: CRC Press.

Hamrick, (2019) *12 STEPS TO MITIGATE CYBER THREATS*, [Online], Available: https://championsg.com/12-steps-mitigate-cyber-threats [12 October 2020].

Lloyd, G. (2020) 'The business benefits of cyber security for SMEs', *Computer Fraud & Security*, vol. 2020, no. 2, pp. 14-17.

Muncaster, P. (2020) *Walmart Sued Under CCPA After Data Breach*, [Online], Available: https://www.infosecurity-magazine.com/news/walmart-sued-under-ccpa-data/ [12 October 2020].

United Nation (2011) *Cybersecurity: A global issue demanding a global approach*, [Online], Available: https://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html [12 October 2020].

Wang, S. (2017) 'Integrated Framework for Information Security Investment and Cyber Insurance', *SSRN Electronic Journal*, vol. 1, no. 1.

1180 words

Reply

Add your reply

Your subject

Type your post

Choose Files No file chosen

Submit

Use advanced editor and additional options

OLDER DISCUSSION
Summary: Need for Cybersecurity

NEWER DISCUSSION
Collaborative Learning Discussion on Initial Post