Launching into Cyber Security June 2022

Home / / My courses/ / LCYS_PCOM7E June 2022 / / Unit 1 / / Collaborative Learning Discussion 1 /

/ Initial Post /

Search forums

Collaborative Learning Discussion 1

Initial Post

Settings

◄ Initial Post

Summary Post ►

Display replies in nested form

Initial Post

by Nomusa Majola - Friday, 24 June 2022, 4:22 PM

COVID-19 , globalisation and digital transformation caused a paradigm shift with regards to the type of cyber threats reported. The industries that experienced an increase in attacks was technology, telecommunications, transport ,manufacturing and distribution sector. It has become critical to preserve confidential information and data integrity. Geo-political tensions have increased supply chain disruptions, which negatively affect economies due to costs involved in avoidance, mitigating and corrective actions.

Despite the physical Russian-Ukraine invasion occurring in 2022, the cyber invasion had long been brewing behind the scenes as early as 2016. Russian covert cyber operations have been targeting Ukraine's infrastructure, financial and energy sector. As a result businesses have suffered greatly due to import/export operations and enforced economic sanctions which trickle over to global economies.

Petya was the first form of malware used, sent as infected email attachments. It prevented hard-drives from rebooting, demanding bitcoin to reverse. Although the Chernobyl Plant attacked using DDos tactics didn't cause immediate damage, moving to a manual system increased operational costs.

Russian forces are still conducting global cyber influencing operations to garner support. To offset and counteract these operations, cyber agencies have started using AI to track and forecast cyber threats. These countermeasures come at a significant cost and have increased cyber insurance rates. The losses can be categorised into 10 classes, namely;

- Intellectual Property
- Business interruptions
- Data loss
- Extortion
- Fraud
- Network failure liabilities
- Breach of privacy
- Reputation
- Asset Damage

- Investigative Costs

Reports estimate that close to $600 billion, nearly 1% of the global GDP, is lost to cyber-crime annually. This makes cybercrime a very lucrative business. Unlike other forms of crime, it has the ability to impact a higher population than any other type of crime and the risk profile to payoff ratio is lower. The increase in availability of digital currency has also made it easier for criminals to be untraceable.

International cyber law enforcement cooperation between countries and the robust adoption of pragmatic orientated approaches will see the cost of cyber-crime reducing. The question is will we be able to stay abreast of the criminals?

https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Andrew, James, and Kenneth Geers. "'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine." *Cyber war in perspective: Russian aggression against Ukraine*. NATO CCDCOE, 2015. 39-48.

Lange-Ionatamishvili, E., Svetoka, S. and Geers, K., 2015. Strategic communications and social media in the Russia Ukraine conflict. *Cyber war in perspective: Russian aggression against Ukraine*, pp.103-111.

Cisco. (2017). *Annual cybersecurity report.* San Jose, CA. Retrieved from **http://www.cisco.com/c/en/us/products/security/security-reports.html**

P.S, Seemma & Sundaresan, Nandhini & M, Sowmiya. (2018). Overview of Cyber Security. IJARCCE. 7. 125-128. 10.17148/IJARCCE.2018.71127.

Mathew Schwartz, “How Do We Catch Cybercrime Kingpins,” Data Breach Today, 2015

Europol, “Internet Organised Crime Threat Assessment 2017,” 2017

Maximum rating: -

Permalink Reply Export to portfolio

Re: Peer Response

by Jacob Dadzie - Monday, 4 July 2022, 12:17 AM

Nomusa you made good point. Following Russia’s attack on Ukraine, the National Cyber Security Centre continues to call on organisations in the UK to bolster their online defences. (Gov.uk, 2022)
The invasion occurs when the pandemic is at its lowest point and people are tired and looking for normalcy. Since so much work is now done online, any disruption to communication networks puts employee productivity in jeopardy. Supply chains are having trouble recovering and will have much greater trouble as a result of restrictions and regional limitations. (Ministry of Defence, 2013)
The production of microchips, which has had trouble keeping up with demand, will suffer from a drop in the supply of raw materials like neon gas and palladium, both of which are largely obtained from Russia. Inflationary pressures will increase across the board, from grocery stores to server rooms, as gas prices climb amid an increasing likelihood of stagflation. Of course, the threat of cyberattacks is still quite real on a global scale.
While the NCSC is not aware of any specific threats that are now posed to UK organisations as a result of events in and around Ukraine, there has been a pattern of cyberattacks against Ukraine in the past that have had an impact on other countries. The wiper software known as HermeticWiper, which is employed against Ukrainian organisations, may also have an effect on organisations abroad. A PC with wiper malware can delete data from the hard disc.
As mention Nomusa ‘The question is will we be able to stay abreast of the criminals?’
UK nuclear power and the NHS are being warned of a Russian cyberattack. In response to the economic crisis, the Russian government's hackers are allegedly attempting to engage in "malicious cyber activities." (the Guardian, 2022)

GOV.UK. 2022. Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion. [online] Available at: [Accessed 1 July 2022].

Ministry of Defence (2013). Cyber Primer. Shrivenham: Development, Concepts and Doctrine Centre.
National Cyber Security Centre (NCSC), 2018). Reckless campaign of cyber attacks by Russian military intelligence service exposed. Retrieved from https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

the Guardian. 2022. UK firms warned over possible Russian cyber-attacks amid Ukraine crisis. [online] Available at: [Accessed 3 July 2022].

Permalink Show parent Reply

◄ Initial Post

Summary Post ►