Peer Responses for Collaborative Learning Discussion 1

Post by **Demian Berisford-Maynard**

Very good points Uvaraj.
It is frightening that it can take around 9 months to identify a breach. The source of your article is IBM, which is probably the worlds number one Information Technology firm. They don't mention if their sample data involved companies utilizing Intrusion Detection Systems. I hope they were referring to companies that don't have proper IDS's in place. That would be an easy way to resolve the issues, for companies to simply implement IDS systems.

If however (much more frighteningly) they were including companies with sufficient IDS systems in place, and that they were inferring that it still takes around 9 months, that would be a much harder pill to swallow, because it would indicated current industry safety measures are a few steps behind the hackers. That would imply its own sets of crucial dillemas, as in how can we improve an IDS conceptually/heuristically to identify breaches as they happen. Are there perhaps ways to lock systems down automatically when their is a breach? These deep critical questions keep me awake at night.

Anyways, I deeply enjoyed your article, and found it very interesting.
Kind regards

Demian

Post by **Kwok Wai Yau**

Hi Uvaraj,

There are very good points about data breaches and the loss of data breaches. The investigation of a data breach is a time-consuming task. On the IT side, it involves tasks like detecting the breach, gathering the evidence, analyzing the breach, and remediation. On the business side, it mainly involves notification. The company needs to notify its stakeholders about the breach. It has to notify their customer when the breach is related to the customer information. Importantly, it has to notify the regulator to report the breach. All are a matter of time such as how much time takes for detection, how much time takes for investigation when to report, what time to report.

As you mentioned, it takes 9 months for detection. IT may need weeks or months for investigation. In consequence, it may cause business delays to notify the related parties. The delay in notifying their customers impacts the organization's image and reputation. The delay in notifying the regulator may cause a penalty on fine.

The blue team in cyber security has to detect fast, act fast, and respond fast. It is always a race to compete time. It is a challenge for all of us. Therefore, many companies implement AI or machine learning to predict and detect attacks and hacks.

Post by **Amit Pahuja**

You made really nice points Uvaraj!

I agree that it takes a lot of time to discover a security breach or a data breach, which is why many organizations are turning to Artificial Intelligence (AI) and Machine Learning (ML) methods of early detection for this reason.

The sooner the crime is discovered, the more time is available for investigation and containment. Every day that a breach goes unnoticed or unaddressed adds to the potentially tremendous costs and risks associated with a data breach.

Educating employees through awareness trainings, implementing a zero-trust framework, and utilizing data encryption are just a few of the prevention strategies available to protect against such assaults.

It appears to me that the vast majority of cyber crimes have taken place in on-premises situations. Because of the rapid use of cloud computing by corporations, public clouds appear to be the next cyber targets, especially given the absence of shared security responsibility understanding between enterprises and public cloud providers such as AWS, Azure, and Google Cloud Platform (GCP).

Post by **Deepak Sidhar**

Some great points made in this discussion by all. The amount of time and cost that goes into detecting a breach and resolving it is vast. There are some great observations on AI and ML being used for cyber security.

After reading this discussion, I was curious to know how many new vulnerabilities were introduced in any given year. I found an IEEE Computer Society publication, which indicated that there were over twenty thousand new vulnerabilities in 2019 and this had increased over 17% over the previous year. Having a team manually trying to detect and investigate each of these will take up so much time and effort.

There is also the argument as to how you prioritise which vulnerability should be investigated first or which vulnerability would have more impact to an organisation, for example the log4j vulnerability (CVE-2022-23307) which was found late last year and Microsoft Excel Remote Code Execution Vulnerability (CVE-2022-21841). Having dedicated teams who know the environment inside out would be beneficial but the sheer

volume of vulnerabilities is overwhelming. Organisations definitely need to consider employing sophisticated tools to help identify a true threat.

Segal, E (N.D.). The Impact of AI on Cybersecurity

https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity
[Accessed 15 March 2022]

Post by **Jonathan Ajodo**

Thank you for your submission which highlighted what governments and other agencies are doing to mitigate the scourge of cyber attacks on businesses. I agree with you that the implementation of government policies and legislations could reduce the prevalence of data breaches. The policies and legislations are required to secure information technology systems, individuals and businesses through requiring them to comply with certain rules and guidelines. It is regulatory compliance, not the existence of these restrictions that prevents cyber attacks. Regulatory compliance improves operational efficiency, reduces legal problems and fosters customers' trust (Srinivas, Das, & Kumar, 2019). Compliance also facilitates information technology systems integration and interoperability.

Regulatory compliance is important to government because consequences such as election interferences and infiltration of key sectors have huge negative impact on national security and citizens' lifestyle. The May 2021 ransomware attack on the Ireland's health system, for example, disabled access to patient records, causing COVID-19 testing to be delayed (hampering travellers who needed the results to make their trips) and cancellation of medical appointments (British Broadcasting Corporation, 2021). The use of third parties and contractors by some government agencies for cyber security systems probably account for their susceptibility to cyber threats. This is more so that the use of third parties opens the door to hackers. Though there is nothing wrong with the use of third

parties, it is necessary that the agencies employ the services of cyber security professionals for the implementation of third party solutions. In other words, third party solutions are not a sufficient substitute for the employment of cyber security professionals in government agencies.

References

British Broadcasting Corporation. (2021). *Cyber attack on Irish health service 'catastrophic'*. Available from https://www.bbc.com/news/world-europe-57184977 [Assessed 21 March 2022].

Srinivas, J., Das, A., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems , 92*, 178-188.