Jul 09, 2020

Cybersecurity Protocols & Resilience Post COVID - Lessons Learnt

lissa coffeey[1]

[1]WP Hacked Help

1 *Works for me* dx.doi.org/10.17504/protocols.io.bidxka7n

WordPress Security Protocols
Tech. support email: **loveneet@wphackedhelp.com**
Click here to message tech. support

lissa coffeey
WP Hacked Help

EXTERNAL LINK

https://secure.wphackedhelp.com/blog/

DOI

dx.doi.org/10.17504/protocols.io.bidxka7n

DOCUMENT CITATION

lissa coffeey 2020. Cybersecurity Protocols & Resilience Post COVID - Lessons Learnt. **protocols.io** dx.doi.org/10.17504/protocols.io.bidxka7n

EXTERNAL LINK

https://secure.wphackedhelp.com/blog/

LICENSE

CREATED

Jul 09, 2020

LAST MODIFIED

Jul 09, 2020

DOCUMENT INTEGER ID

39063

DISCLAIMER:

DISCLAIMER – FOR INFORMATIONAL PURPOSES ONLY; USE AT YOUR OWN RISK

The protocol content here is for informational purposes only and does not constitute legal, medical, clinical, or safety advice, or otherwise; content added to protocols.io is not peer reviewed and may not have undergone a formal approval of any kind. Information presented in this protocol should not substitute for independent professional judgment, advice, diagnosis, or treatment. Any action you take or refrain from taking using or relying upon the information presented here is strictly at your own risk. You agree that neither the Company nor any of the authors, contributors, administrators, or anyone else associated with protocols.io, can be held responsible for your use of the information contained in or linked to this protocol or any of our Sites/Apps and Services.

Citation: lissa coffeey (07/09/2020). Cybersecurity Protocols & Resilience Post COVID - Lessons Learnt. https://dx.doi.org/10.17504/protocols.io.bidxka7n

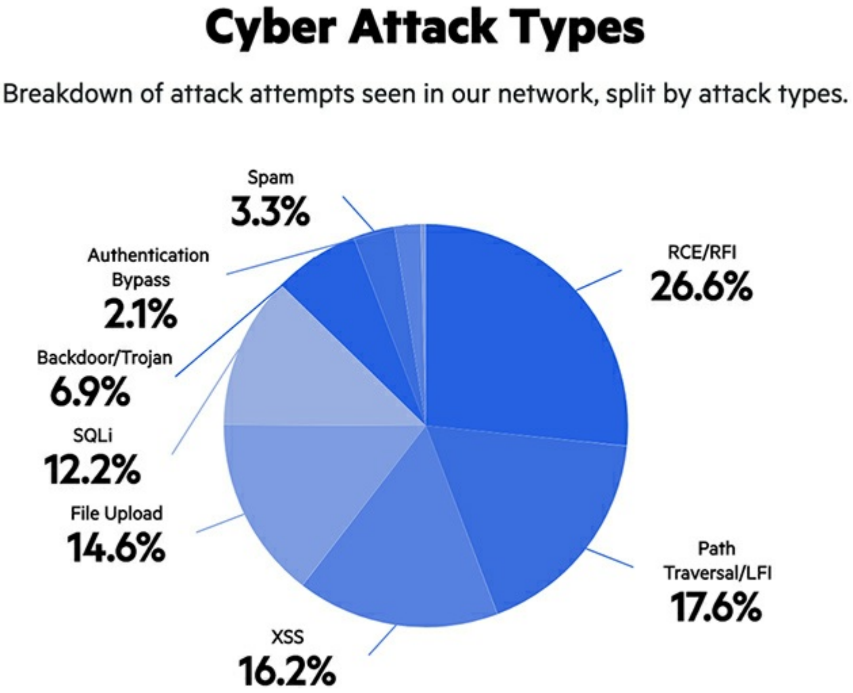
Equivalent situations to those described with respect to the pandemic regarding deficiencies in the collecting and reporting of data show up in the case of cyberattacks and data breaches. Reported cyber incidents likely represent only a small fraction of the actual total, and extrapolations to totals are merely guesswork, in my opinion. Consequent decisions as to how to mitigate cyber risks are based on shaky "facts," and investments in cybersecurity are likely much lower than they would be if the true extent of attacks and compromises were known and released. We are talking order(s) of magnitude here also.

Why Protect the Data?

Whether your company is in a highly regulated industry such as health care, government or finance, data privacy legislation is in place that mandates how data is secured and involves hefty fines if leaks were to happen. Whether it is GDPR or one of the U.S. state laws such as CCPA, your company must be able to safely retain records, archive emails and perform discovery tasks.

A strong cyber resilience plan maintains data retention policies and automated backup practices for full compliance.

There have been significant changes in web attack and traffic trends as a result of COVID-19,

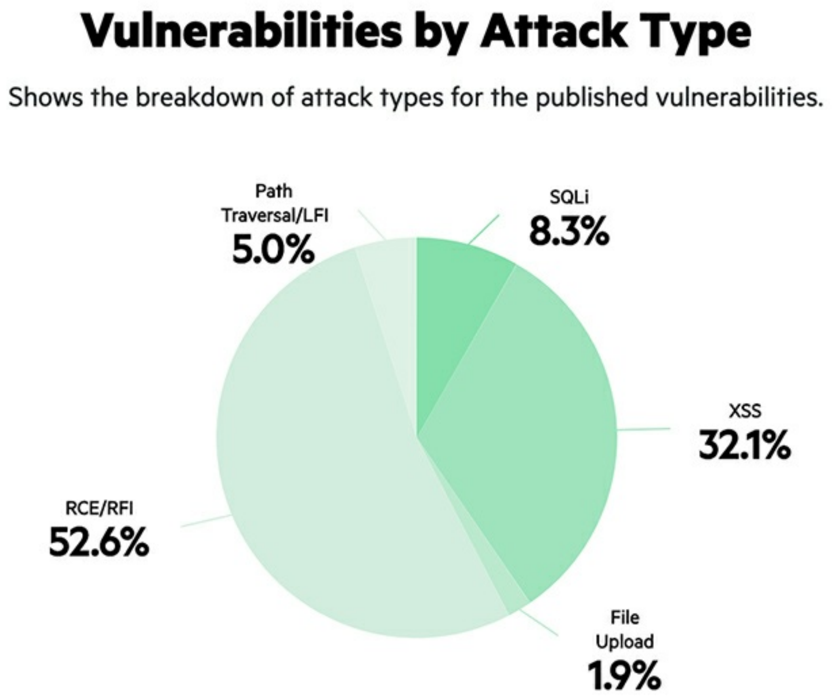


cyber attack types

Amid COVID-19, web traffic and attack trends were affected. During the month of March, changes in traffic and attack trends were tracked across multiple industries and countries as the coronavirus pandemic escalated.
The March findings indicated that the food and beverage industry experienced more website attacks globally (+6%), especially in Germany (+125%). There were more attacks on the financial industry both globally (+3%) and in specific countries like Italy (+44%), UK (+21%), and Spain (+18%).

Financial services suffer the most from XSS attacks Cross-site-scripting attacks, a type of malicious script injection, were the most dominant attack vector (32%) for sites in the financial services sector. This may be because taking over web sessions in financial sites is extremely profitable for hackers, or because of the high regulation on these sites and the frequent risk assessment and penetration tests being conducted.

Citation: lissa coffey (07/09/2020). Cybersecurity Protocols & Resilience Post COVID - Lessons Learnt. https://dx.doi.org/10.17504/protocols.io.bidxka7n



cyber attack vulnerabilities

Cyber Resilience Post COVID: More Important Now Than Ever Before

The critical need for a business resilience strategy can be summed up in one word: coronavirus. This global pandemic has changed the way businesses operate presently and likely into the future. For companies that are struggling to maintain business continuity, a resilience strategy is essential to keep employees connected and data protected and meet regulatory compliance guidelines.

Cloud services are a great resource to provide collaboration and automated data protection as it also supports mixed IT environments. Endpoint data protection ensures that desktops, laptops, tablets and smartphones are secured against ransomware and other malware. But regardless of the technologies or strategies you have in place, it is worthless unless it is tested. Only when a plan is enacted do businesses uncover the vulnerabilities or issues they hadn't considered before. Testing helps to uncover these issues and educates employees on the proper procedures prior to a real-life issue. And even as we all work from remote locations, now is a good time to find those weaker spots and implem
ent best practices.

While an organization may not have a formal plan in place now, current events have shown that it is best to start building one that can be used in the coming weeks or put in place prior to the next big crisis. Whether it is a small, localized issue or larger global concern, it is critical to have a cyber resilience plan to handle all the different protection layers.

Obfuscation

I have maintained all along that cyber incidents are far greater than the numbers and sizes reported and published. My guess was an order of magnitude, but that may be way too low. There are several reasons for this.

There is strong motivation for obfuscation by victim organizations as well as cyber defenders. Based on my observations, some victim organizations seek to avoid the number and size of successful cyberattacks that are publicly revealed so as to limit their exposure to lawsuits and damage to their reputation. Organizations will seek legal interpretations of whether an incident is considered a reportable breach. Even when reported, some victims of cyberattacks and data breaches do not see much publicity. Perhaps some publicity depends on whether a reporter is privy to notifications of breaches.

Those companies in the business of defending organizations against cyberattacks appear to prefer overstatements. In one of few

Citation: lissa coffeey (07/09/2020). Cybersecurity Protocols & Resilience Post COVID - Lessons Learnt. https://dx.doi.org/10.17504/protocols.io.bidxka7n

instances when such obfuscation is mentioned in print,[i] the authors claim that "… the growing volume of threatening statistics … are very often made by cybersecurity industry participants who will undoubtedly profit from increase in cybersecurity spending."

The lesson from the pandemic is that data, manipulated for political and personal reasons, yields heavily-biased results that used to further the interests of different groups. Such decisions are likely to be unhelpful at best and dangerous at worst. We need clean, unbiassed data if we are to make headway in mitigating cybersecurity risk.

Falsification

Deception is an integral tool of both attackers and defenders. Cyberattackers will try to conceal the source of the attack for any number of reasons. They may fear retribution, or they want victims to direct their responses to other parties. Whatever their motives, they might masquerade as another player (i.e., spoofing) or will use readily-available Dark Web tools so as to appear anonymous.

Potential victims will try to misdirect attackers using such tools as honeypots where the attackers believe that they have hit paydirt only to discover that they were served false data as defenders work on capturing information about the attacker and forming and implementing some type of response. They may also use SQLInjection to inject malware in websites. Another widespread hack attack commonly seen is Pharma hack wherein hackewr injects links to shady pharmacuitical websites with sole intent to steal financial information or sell illegal drugs. Wordpress sites are the most common source of such kind of hack attacks.[ii]

Again, falsification has its place, particularly when used defensively. But misinterpreting the source of attacks (or the origins of a pandemic) can lead to reactions against innocent parties and potential broader conflict, all based on a misunderstanding. The lesson here is to be particularly fastidious when discovering sources forensically and when making accusations against possible attackers.

Testing & Scanning

Testing in this context, is usually termed "monitoring." Many cyberattacks are never discovered by victims. Third parties, such as law enforcement, business partners, clients and customers, security consultants, or regulatory overseers, are often the ones. who make the discoveries and report back to the victim organization, which often doesn't have a clue as to what happened, or when and how the incident occurred. Second, many known breaches are never disclosed by victim organizations due to reputational concerns or, if they are, the announcement doesn't reach the popular press, as described in the obfuscation section above.

It is clear from published reports about data breaches that monitoring is sadly lacking generally and it is particularly disturbing when the victim organization is a seemingly high-tech force such as the CIA. This distressing reality is brought out in a recent article.[ii]

The lesson here is to make mandatory comprehensive monitoring of activities within systems and networks. If a serious standard is established and organizations are encouraged (or forced) to adhere to that standard, many more cyberattacks will be observed and stopped, or at least mitigated.

Sampling

When it comes to reports that show the number and percentage of attacks, along with all manner of other details, we see that the sample size is minute compared to the actual population of potential victims.
An immediately-apparent characteristic of free online reports is their inconsistency, followed by small sample size, self-selected data sources, limited breakdown of data, and differing data categories. While not necessarily applicable to all the studies, perhaps among the most revealing set of limitations are listed on page 74 of the ***Ponemon/IBM 2019 Cost of Data Breach Report***,[iii] as follows:

- **Non-statistical results**—The data were not collected in a scientific manner and therefore cannot be used for statistical inferences
- **Non-response**—The data were collected on a small sample without testing for non-response bias
- **Sampling-frame bias**—The sampling-frame was believed to be biased towards companies with more mature privacy and security programs
- **Company-specific information**—Since the information collected was sensitive and confidential, company-identifying data were not collected
- **Unmeasured factors**—To keep the interviews simple and concise, other important variables, such as leading trends and

Citation: lissa coffey (07/09/2020). Cybersecurity Protocols & Resilience Post COVID - Lessons Learnt. https://dx.doi.org/10.17504/protocols.io.bidxka7n organizational characteristics, were omitted with the consequence that significant variables may have been missed

- **Extrapolated cost results—**It was possible that the respondents did not provide accurate and truthful responses and that the cost extrapolation methods may have introduced biases and inaccuracies.

Given all these disclaimers, it would appear to be virtually impossible to get the entire picture. As with coronavirus testing, the number of incidents will increase as sample size increases, but the ratios, or metrics, do not necessarily increase in the same way. Indeed, the numbers may fall. There are scientific methods for determining appropriate sample sizes and calculating the levels of confidence in the results. Why not use them? We shall look at the lessons to be learned in the area of metrics in a future column.

[i] Paul Rohmeyer and Jennifer Bayuk,***Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions***, Stevens Institute of Technology Quantitative Finance Series, Springer Apress, 2019. Foreword by Dr. Larry Ponemon.

[ii] Wordpress security team, “ Understanding, Diagnosing And Fixing WordPress Pharma Hack by cleaning up the database and infected files.” ***CNN***, June 16, 2020. Available at https://secure.wphackedhelp.com/blog/wordpress-pharma-hack-fix/

[iii] Zachary Cohen and Alex Marquandt, “CIA cyber weapons stolen in historic breach due to ‘woefully lax security’, internal report says,” ***WP Hacked Help***, June 1 , 2020 [updated]. Available at https://www.cnn.com/2020/06/16/politics/cia-wikileaks-vault-7-leak-report/index.html

[iv] Available via https://www.ibm.com/security/data-breach Requires registration.

Citation: lissa coffeey (07/09/2020). Cybersecurity Protocols & Resilience Post COVID - Lessons Learnt. https://dx.doi.org/10.17504/protocols.io.bidxka7n