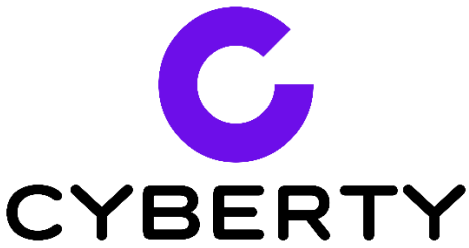

Threat Reduction

Your Cybersecurity Strategy for 2020 – in 5 steps

#CyberNorth 2020 edition

https://cyberty.io

Essential Cybersecurity tips for businesses

1. Know What You Have

When working with our customers, we find there's this tendency to over-invest in many technologies, particularly, whatever the shiniest solution is at the time. Organizations end up in a situation where they have a range of technologies but they've often never fully implemented them or optimized them to the full potential. When we go in from an audit perspective, we'll often find that there are massive gaps in an organization's maturity, and the gaps aren't there because they're lacking solutions, they're there because they're not using the solutions that they have to their full extent.

The fact that there is a possibility to get a lot more value out of your current solutions without spending a lot more money is something that organizations really need to take advantage of.

2. Back Burn Your Environment

Back burning, or 'hazard reduction burns' – take the opportunity to do a controlled removal of leaves and sticks and dry material that could potentially be a threat when things are bad.

Many times, data doesn't have an owner, is out of date, or stored in antiquated systems. All of this presents a significant exposure to data breaches (not to mention GDPR fines). By back burning your environment, you'll look at what you have in place and get rid of the data that is basically presenting an exposure without any real benefit to you. You can reduce the 'hazard' of data being breached, simply by no longer holding that data.

3. Patch Patch Patch, Update

Everything is vulnerable now or it will be in time. Make sure to update everything in your organization. Software, firmware & hardware, operating systems IOT/OT and anything and everything that your organization is using. One recommendation that we give to smaller organizations is to simply keep an inventory of IT systems owned by the organization. Make sure that none of the systems have reached end of life and no longer supported. If you find such systems, replace them or make sure to isolate them from internet access (www.shodan.io) is the search engine that will help you to make sure that you are not exposed).

Make sure to update and patch everything IT related to minimize the risk of information leaks, breaches, hacks and financial and legal penalties.

4. Get Help

Trying to get a multiplier on the security investment that you've already spent or will spend. If you accept the fact that we all have limited resources, if you can get a two to three times return on what you're spending, then it makes a massive difference to a security program. That multiplier effect will come from things like managed security services. The sharing of the significant capital cost and finding a way to get a better return on that. Looking at how you start to use external expertise and collaboration platforms.

5. Measure, Communicate and Educate

Metrics are always going to be a challenge. The reality is that cybersecurity is a complex area. Even if you look at the points we've talked about so far, how would you define a metric that points to the risk that you've reduced through back burning an environment? You can talk about how much less data and exposure you have, but it doesn't guarantee that you won't have a breach. With all these things, the challenge is that the people who are asking for the metrics and the reporting, they want something that gives them comfort that they won't have an incident occur.

Whereas from the perspective of a security leader, really the message is that we can't deliver that assurance, but can demonstrate that we are making good decisions and have a mature program in place that effectively manages the risk. But the risk is not going to be zero. Having a metrics approach that is discussed and agreed upon as far as what it represents for the practitioners that put it together and the business leaders that will receive it is the best way forward.

Having a discussion up front about your metrics and what they're communicating as it relates to the business and the security program itself is key.

Last but not least educate yourself and your employees, employee awareness is key. Given today's evolving threat landscape, collaborating with other security leaders is essential to support the effectiveness of your current security strategy.

For more information about this material contact hello@cyberty.io

Thanks to all participants, speakers and partners!!!

Speakers from:

Volvo Cars, Cyberty, IBM Security
Swedish Cybercrime Center (SC3), Swedish Internet Foundation

Media coverage:

Norrbottens Kuriren, Norrländska Socialdemokraten, Tidningen Extra,
SVT Norrbotten: https://www.svt.se/nyheter/lokalt/norrbotten/norrbotten-daligt-rustat-mot-cyberhot
SR – Eftermiddag i P4 Norrbotten

See you next year @ CyberNorth 2021!

https://cybernorth.se