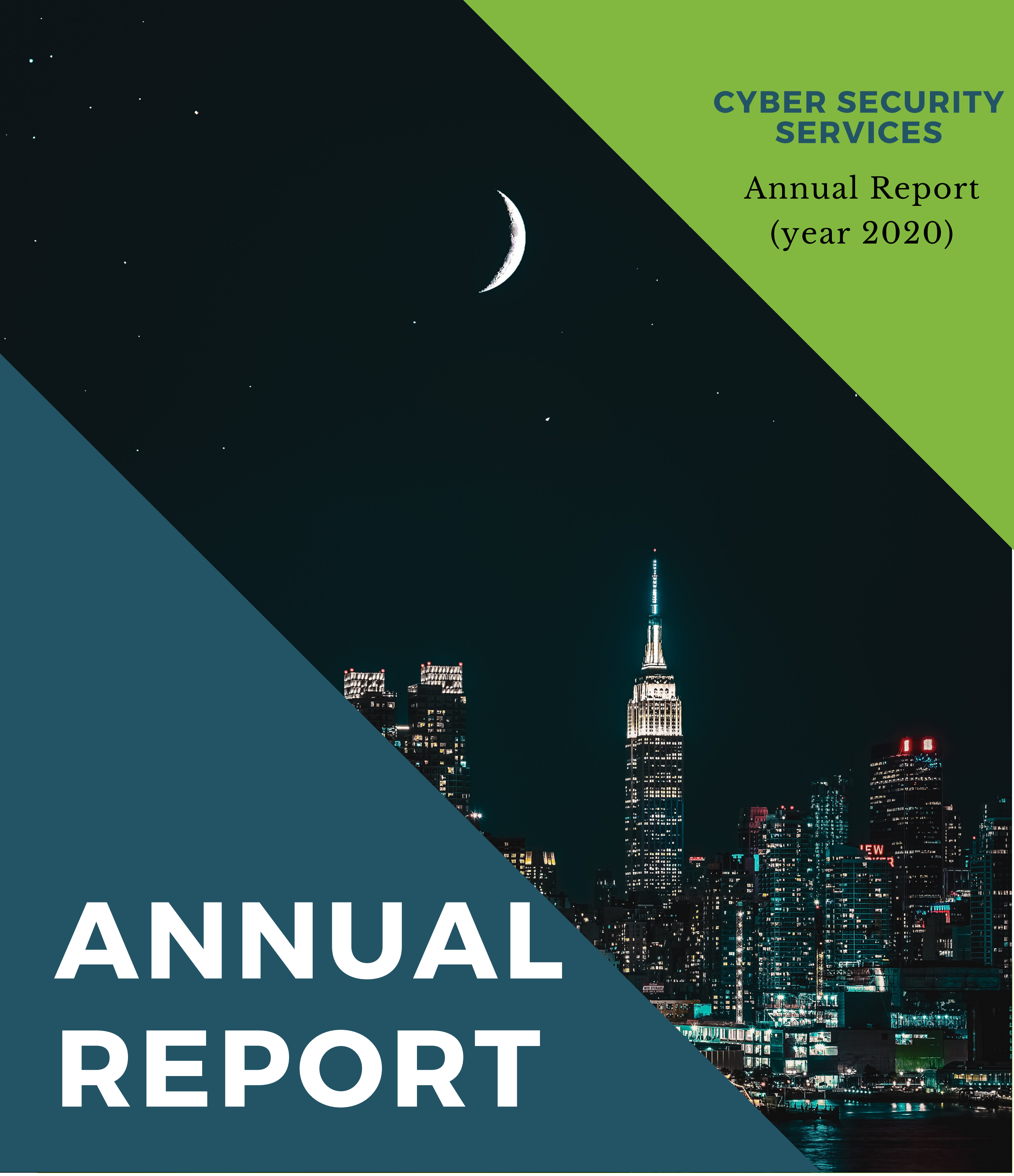


CYBER SECURITY SERVICES

Annual Report
(year 2020)

ANNUAL REPORT

PREPARED BY

Prashant Phatak
Chetna Pangare

Valency Networks
Its all about Ethics

AUTHORS

Prashant Phatak
Founder, CEO - Valency Networks

Chetna Pangare
CIO, CISO - Valency Networks

Disclaimer
Statistics presented in this report are an outcome of cyber security services data gathered by Valency Networks. There is no data in this report that is copied from or referred from any other source on internet or otherwise. Feel free to refer to this report and use information contained in it for your presentation. Although, since this report is a copyrighted material of Valency Networks, modification or presentation of this report without prior consent of Valency Networks is strictly prohibited. You can contact us using the details found on our website link (mentioned on the last page of this report).

YEAR 2020: NOT JUST COVID

Cyber Security Report

Soon when the world went in lock down during pandemic all the business around world made strategies to ensure business continuity and not many but few focused their efforts on security as well.

During pandemic all IT and non-IT industries focused on security in employee connecting to company networks remotely or remote accessing of networks. But critical components missed out were:

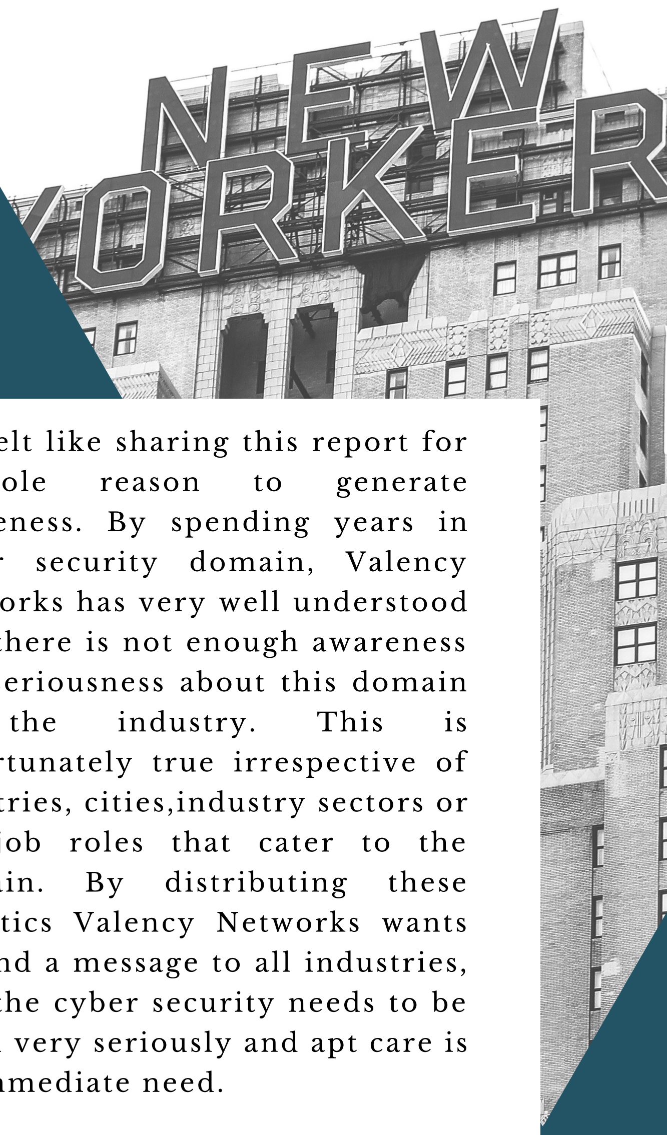
- Data at rest and
- Data in transit

All business and companies use various applications and tools either 3rd party or self-developed. Think of an in-house developed project collaboration and project management tool hosted either on a local server or Cloud. In pandemic hackers were luring for data stealing like bees for honey in spring. And while industry was focused on securing VPN and other technical fixations, what was left easy and unprotected for hackers were following attack vectors that lead to web hacks network hacks and cloud exploitation.

- Insecure and vulnerable web application
- Unpatched and un-hardened web server
- Unreliable certificate deployment on web server
- Unauthenticated exposed API's
- Malicious or not-in-use services running on server on cloud

a year's overview

WHAT THIS REPORT IS ALL ABOUT?



"We at Valency Networks cater to a variety of services to our customers, ranging from vulnerability assessment and penetration testing to information security compliance services.."

With a global base of great customers, we end up finding a great deal of security issues and security postures of their organizations.

This report contains a gist of all those findings. We took a great deal of samples from all the testing performed in the year 2020, such as VAPT of Web applications, static security analysis of Android and iOS applications, Exploiting of network infrastructure and ISO27001, HIPAA, GDPR, and SOC2 related vulnerability assessments etc.

We felt like sharing this report for a sole reason to generate awareness. By spending years in cyber security domain, Valency Networks has very well understood that there is not enough awareness and seriousness about this domain in the industry. This is unfortunately true irrespective of countries, cities,industry sectors or the job roles that cater to the domain. By distributing these statistics Valency Networks wants to send a message to all industries, that the cyber security needs to be taken very seriously and apt care is an immediate need.

This report does not contain any ready-made material from internet or any other survey. It is generated by using the factual data gathered by Valency Networks, while catering to its customers. The numbers, graphs and statistics shared in this report are copyright of Valency Networks. As a reader you are encouraged to read, understand and follow this report for your own benefit, and get a consent of Valency Networks if you want to use material and data contained in this report, for your own reporting or any other purpose of presentations.

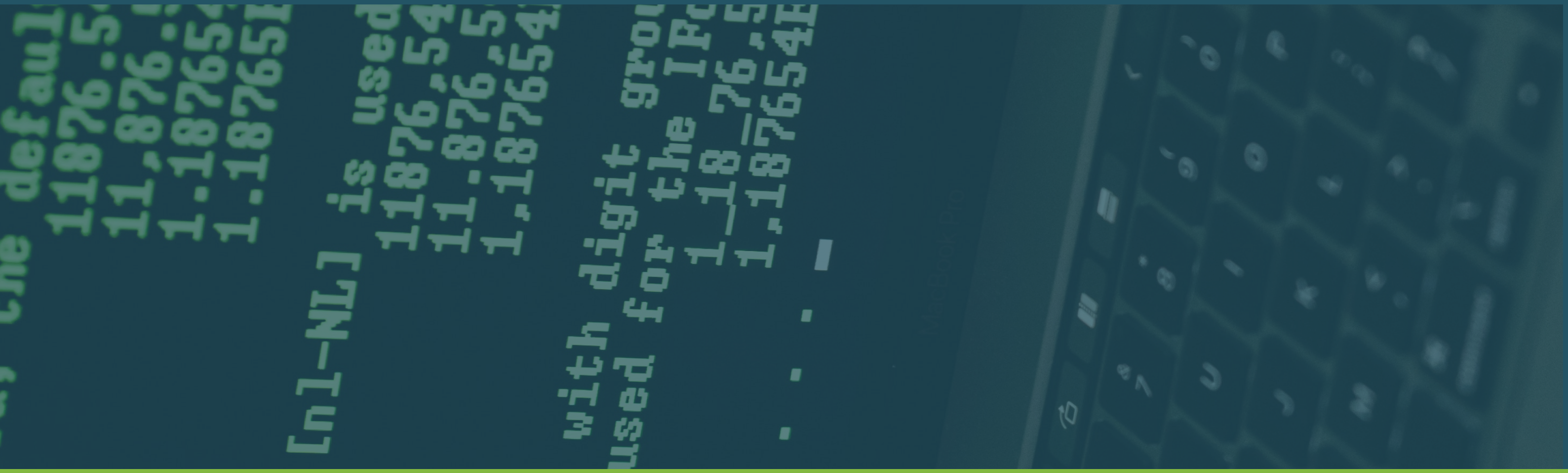
CYBER SECURITY LEARNING THIS YEAR

Year 2020 was a strange and yet very educating year for cyber security professionals. Due to COVID19, all industries started being introspective about their own cyber security posture. It was also a sharp learning curve for Valency Networks. A Top 10 cyber-attacks gist as seen by Valency Networks team is mentioned below:

- Web applications saw new types of attacks which are beyond the ones listed on OWASP Top-10
- Web server level attacks increase exponentially, in order to take control of the entire server
- Companies because more serious about ISO27001 and ISO13485 compliance's
- Fintech companies saw higher rate of REST API injection type of attacks
- Healthcare companies saw increased rate of Android app based attacks
- Internal patching is still a big problem for vulnerabilities within a LAN
- Corporate networks saw more attacks on the VPNs and firewalls
- Loose firewall policies helped attackers spread ransomeware
- Firewall rule bypassing increased to a large extent
- IoT attacks increased to some extent

KEY TO A BETTER CYBER SECURITY ASSURANCE

Keeping technical observations away, following learning are also important



- Cyber-attack are not restricted to IT industries but we saw financial services, retail, manufacturing, healthcare, professional services been victims in 2020 and can be targets in 2021 too.
- Cyber-security should to be a CEO, CFO level matter and not just IT or Cloud Ops
- Advanced risk analysis and monitoring methodologies is need for every business
- Email literacy needs to be uplifted, since with pandemic our lives have gone online more than ever before
- Weak end-point protection can hit big on pockets along with negligence towards Cloud and network can bring-in law-suit or reputational damage

last year's

WEB ATTACKS

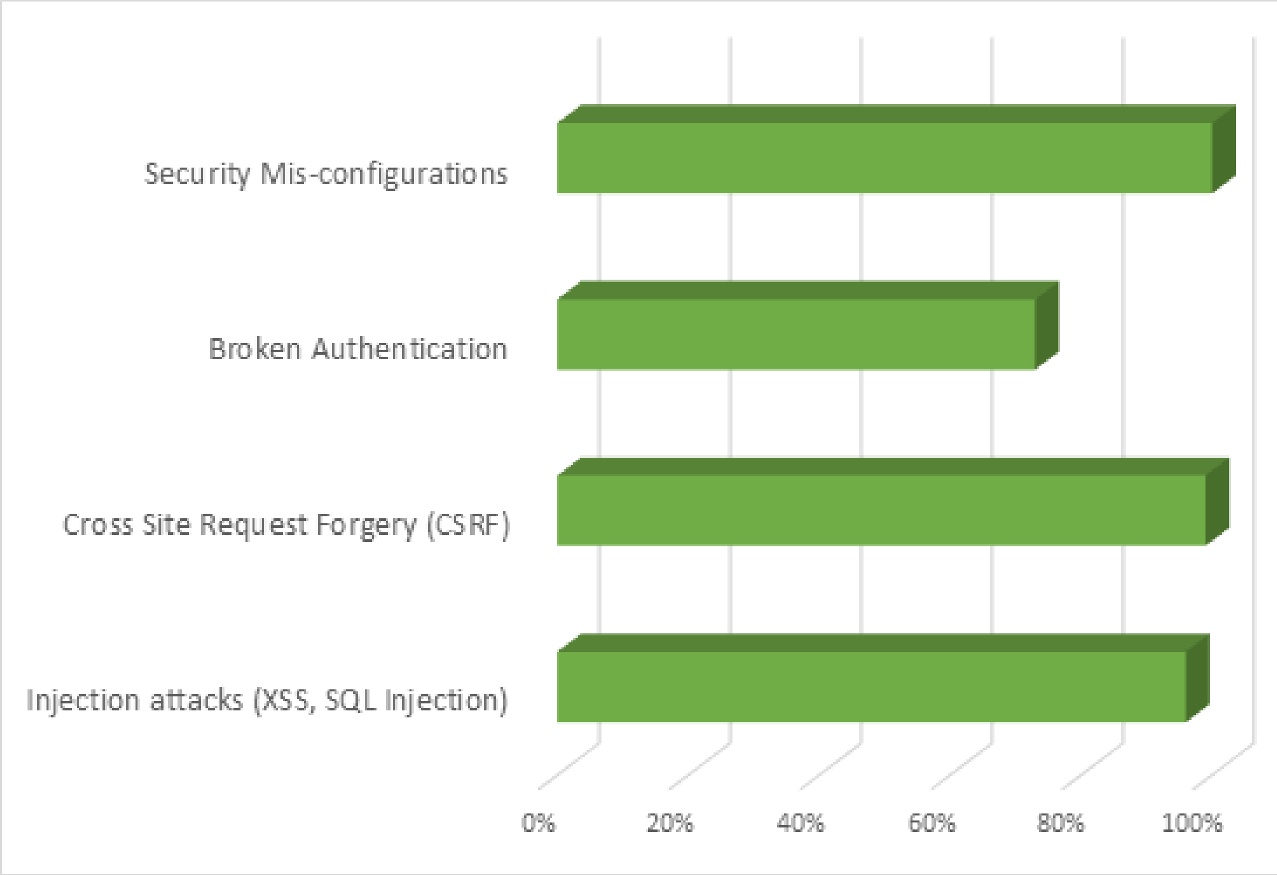
NUMBERS & STATISTICS

96%

XSS &SQLi

99%

CSRF



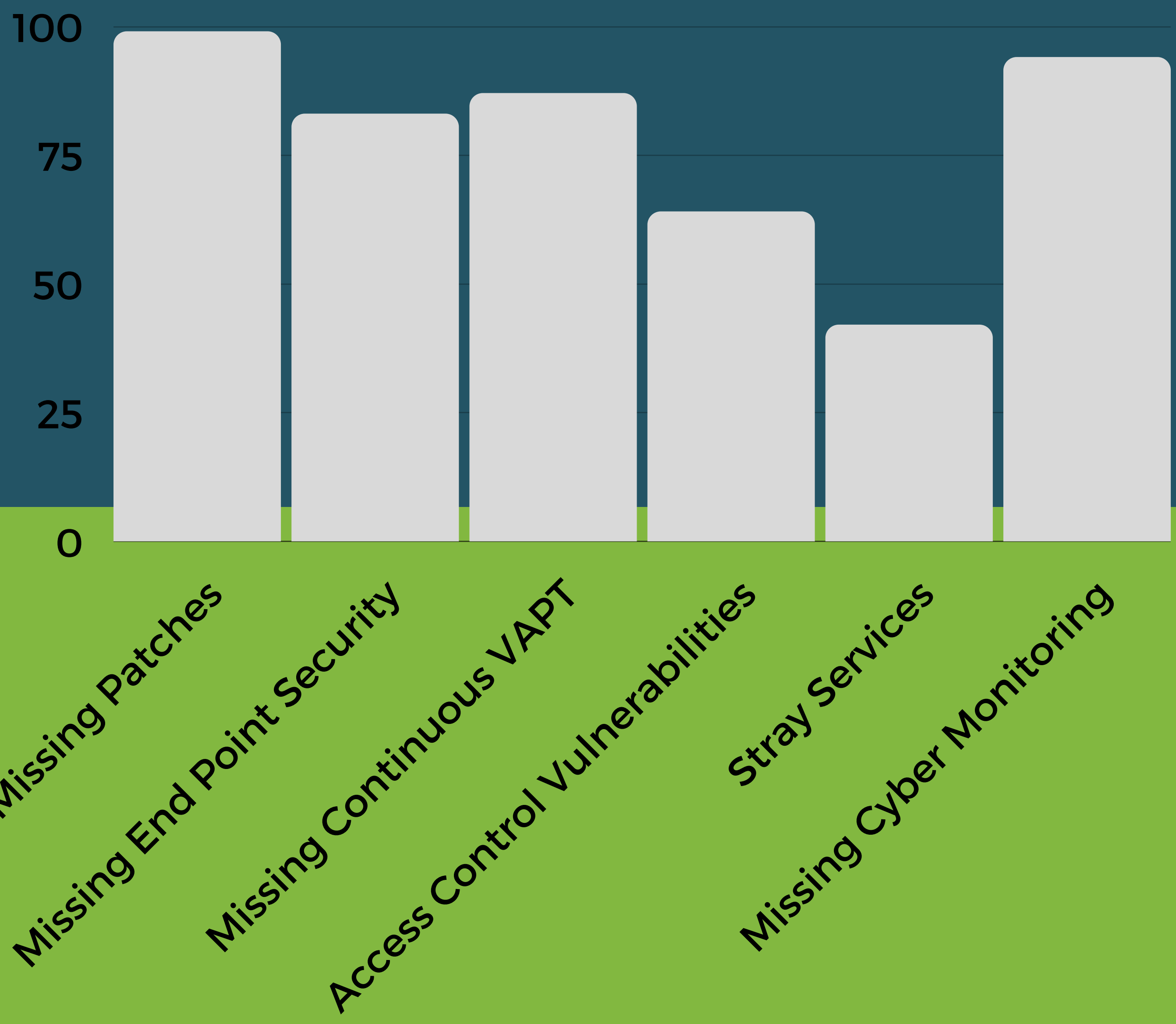
last year's

SERVER ATTACKS

NUMBERS & STATISTICS

99%
Missing Patches

42%
Stray Services



TOP 5 VULNERABLE PORTS

TCP 443
SSL

TCP 22
SSH

TCP 21
FTP

TCP 1433
MSSQL

UDP 500
VPN

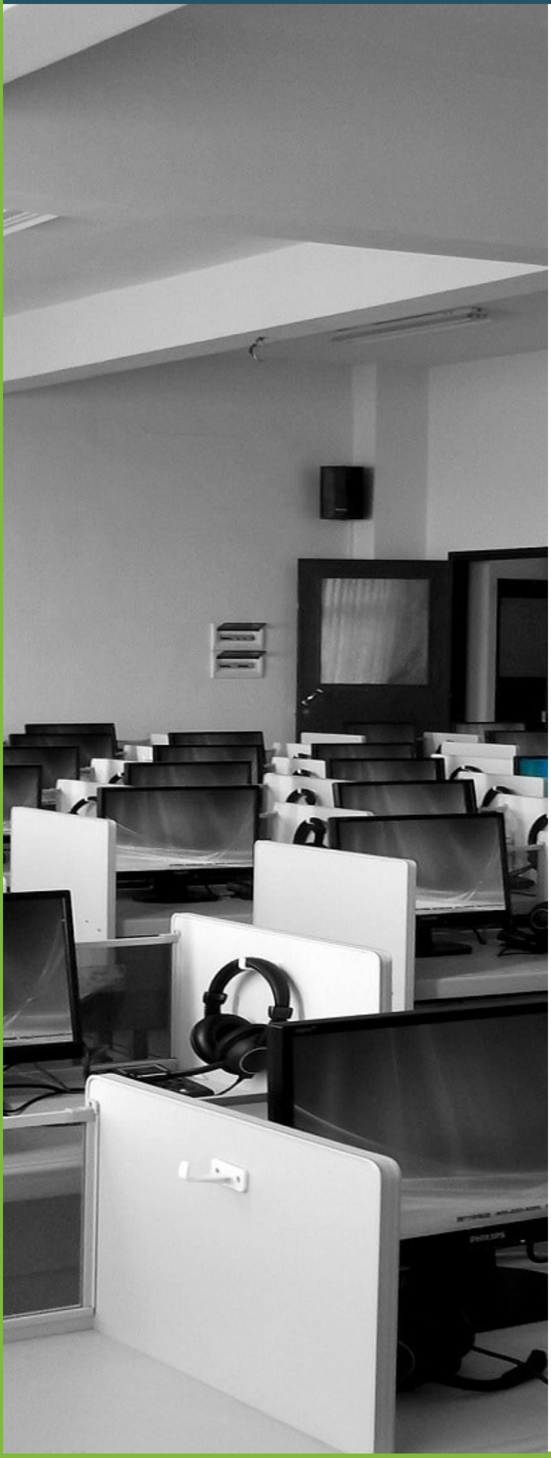
a year's overview

WHICH INDUSTRIES GOT ATTACKED THE MOST?

Below is a list of industries whom we catered to for cyber security services. The list is in the descending order, which means that the first industry sector in the list was the most hacked one.

- Manufacturing industries going for IoT implementation
- Healthcare industries creating medical devices and software
- IT Product companies hosting their SaaS applications
- Fintech companies having their mobile applications
- IT Services companies who remote into their customer’s infrastructure

WHAT SHOULD ORGANIZATIONS DO TO BE CYBER RESILIENT?



Do not hide behind tools i.e. IDS, IPS or DLP. Most basic and apt thing to do is communicate with all your employees about cyber-security and being cyber resilient. Every two out of three businesses saw insider attack and threats in year 2020. Being communicative on cyber incidents and providing pointer on how to protect or prevent against cyber-incidents makes employee more on-guard and watchful!.

Your list of actionable To-Do for being cyber-secure resilient:

1. Be Communicative about latest cyber-fraud & share protection against them
2. Enable 2 Factor authentications more
3. Secure your WiFi, VPN, LAN/WAN networks for data in transit

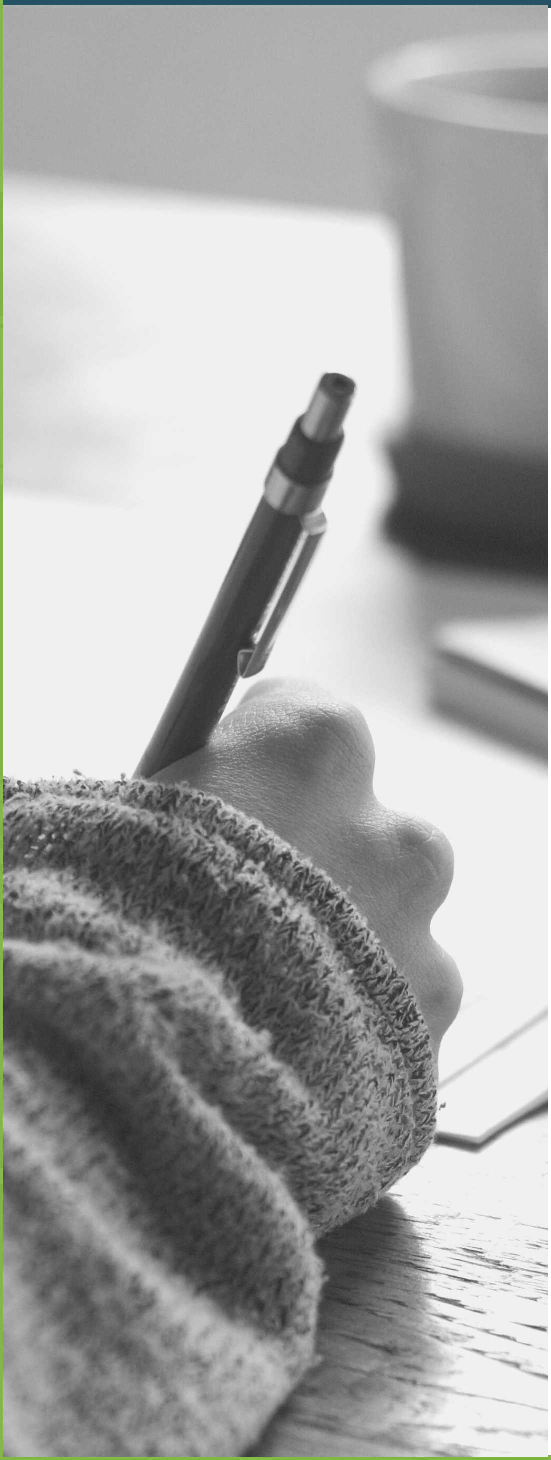
ADDITIONAL SURVEY

Phishing attacks are increasing drastically. Valency Networks gets many requests of cyber forensic cases to handle wherein the root reason is phishing. A great deal of phishing awareness is required.

Ransomeware attacks are increasing too. Most of those are stemming out of incorrect firewall configuration, and inadequate patching. A good discipline via ISO 27001 compliance is required to be implemented

Cloud server attacks were found to be at its maximum in 2020, as analyzed by Valency Networks team. Most of the attacks were due to incorrect or missing cloud infrastructure configuration that resulted into stealing of data by attackers.

WHAT THIS YEAR TAUGHT US?



Year 2020 was a roller-coaster ride for sure. It certainly taught us many thing in our professional and personal life, such as below:

- When we are working from home, its important to remember that hackers are also working from home, and with the same enthusiasm.
- Cyber security starts at management level in any organization. A correct strategy and adequate funding is important to ensure that the business runs without any glitches.
- Healthcare sector and IoT have a lot to do besides just the vulnerability assessment and penetration testing or implementation of HIPAA or GDPR.
- A pandemic such as COVID19 is certainly a problem to the humanity but it is also an opportunity to look at our own cyber security at a personal level, and also that of our family. This boils down to whether we are using safe web applications or mobile applications, is our personal data safe, are we enough aware about phishing and whaling attacks etc.

REFERENCES

Why Manufacturing Industry is Prone to Ransomware Attacks?
(https://www.valencynetworks.com/blogs/why-manufacturing-industry-is-prone-to-ransomware-attacks/)

Why Hackers Like The Healthcare Industries?
(https://www.valencynetworks.com/blogs/why-hackers-like-the-healthcare-industries/)

Vulnerability Assessment – Automated v/s Manual Testing
(https://www.valencynetworks.com/blogs/vulnerability-assessment-automated-v-s-manual-testing/)

Top 5 Reasons To Perform VAPT Of Your Web Application
(https://www.valencynetworks.com/blogs/top-5-reasons-to-perform-vapt-of-your-web-application/)

GDPR Compliance for Mobile Apps
(https://www.valencynetworks.com/blogs/gdpr-compliance-for-mobile-apps/)

Why HIPAA and GDPR cannot replace each other?
(https://www.valencynetworks.com/blogs/why-hipaa-and-gdpr-cannot-replace-each-other/)