Let's talk about Cyber Security 101

By Jess Kelfkens and Carel Krogh

Top 3 business risks 2022

Globally

Cyber incidents [e.g. cyber crime, IT failure, data breaches etc]
Business interruption [incl. supply chain disruption]
Cyber risk was the most feared cause.
Natural disasters

Food & Bev

Cyber incidents
Business interruption
Climate change

South Africa

Cyber incidents
Business interruption
Critical infrastructure blackouts

Allianz Risk Barometer report 2022.

Cyber Incidents

- Top business risk in 2022 globally.
- Ranked first in 15 countries, incl SA
- Trends in recent cyber attacks include double extortion, supply chain software vulnerabilities, & targeting physical critical infrastructure.
- The main driver is the recent surge in ransomware attacks.

Frameworks to manage Cyber Risk

• NIST	https://www.nist.gov/
• ISO27000	http://www.27000.org/
• COBIT	https://www.isaca.org/resources/cobit
• CIS controls	https://www.cisecurity.org/

Consider Regulatory Frameworks

• POPI	https://popia.co.za/
• GDPR	https://gdpr-info.eu/
• PCI-DSS etc	https://www.talend.com/resources/pci-dss/

References

- https://www.foodfocus.co.za/home/Industry-Topics/Risk-and-Governance/Demystifying-incident-response-plans
- https://www.foodfocus.co.za/home/Industry-Topics/Risk-and-Governance/Demystifying-incident-response-plans
- Allianz Risk Barometer 2022. {2022}. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2022.pdf
- Top 10 Most Common Types of Cyber Attacks. [n.d.]. Retrieved January 23, 2022, from https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
- Types of Cyber Attacks: 10 Widely Known Cyber Attacks [UPSC S&T Notes]. [n.d.]. Retrieved January 23, 2022, from https://byjus.com/free-ias-prep/types-cyber-attack/
- NCSC. [n.d.]. NCSC Glossary. Retrieved January 24, 2022, from https://www.ncsc.gov.uk/static-assets/documents/NCSC_glossary.pdf
- BSI. [n.d]. Glossary of IT security terms - Protecting networks, computers and data | BSI. Retrieved January 24, 2022, from https://www.bsigroup.com/en-GB/Cyber-Security/Glossary-of-cyber-security-terms/

Common Cyber Attacks

Malware
- A form of application that performs nefarious activities.
- Some are designed to create network access, spy on credentials or simply disrupt destroy or hold data hostage.
- Further, includes viruses & worms and ransomware that holds data hostage

Phishing
Where an attacker tricks an unsuspecting target into handing over valuable information, such as passwords. Common form of cyber attack due to its effectiveness & simplistic execution pattern. Usually via email, websites SMS etc.

SQL Injection
This cyber attack targets specific SQL databases. In case permissions are not set properly, a hacker can manipulate SQL queries into changing the data if not deleting them altogether. The least-privileged model is advantages here.

Distributed Denial-of-Service [DDoS]
Attack is designed to overwhelm the resources of a system, disrupting it so its unable to reply to legit service requests. May lead to services slowing down on the website until it eventually crashes. Unlike denial-of-service attacks [DoS] , DDoS uses multiple compromised devices to bombard the target server, which sophisticated firewalls cannot respond to.

Man-in-the-middle attack
A message interception breaches in cybersecurity between 2 parties that make it possible for an attacker to access data sent between 2 people, networks, or computers. Data encryptions prevent third parties in intercepting or tampering data transmitted in the network.

Business Email Compromise [BEC]
- Designed to access critical business info or extract money through email-based fraud. Can cost a company millions. Hackers target employees with authority to do business transactions, tricking them into transferring money into the hacker's account. BEC attacks are common & damaging.
- Hacker embeds malicious code [malware] into a website which when visited infects the visitors device with malware. Malware will steal data or crash the system.

DNS Tunnelling
Cyber attack that encodes the data of other programs, provides attackers with a stable line of communication to the target. Chances are that firewalls won't be able detect such an attack.

Common basic security controls to implement now

Backup data regularly
• Consider data privacy regulations as a guide in terms of specific controls required
• Backup rule of 3
• At least 3 copies of your data.
• Stored on at least 2 media types.
  1 copy stored off-site.

Restrict remote access to your network
Consider installing VPN that will secure & encrypt communication data

Create a complete asset inventory
Include hardware, [i.e. computers, printers, network devices], software, & data storage locations.

Email safety
• Scan all emails for malicious links & attachments, using anti-virus software.
• If a hosted services provider is used. Obtain a list from the provider of controls implemented as part of the service, to determine the extent of reliance to place on those security controls.
• Humans are the weak link, so as part of email security awareness communicate to all staff to:
  • Not click on links received through email.
  • Verify the reply-to address before engaging with the sender.
  • Not download files or open attachments from unknown senders. Protect personal info [user names, passwords etc.].
  • Legit businesses will not send an email asking for sensitive personal info.

Apply software and hardware patches
• Keep this updated
• Automate where possible.
• Test patches before rollout if possible.

Monitor your network
Detect anomalies or signs of possible compromise

Incident response plan
• Detail instructions to detect, respond to, & recover from network security incidents.
• Must be a living document
• Test & review regularly

User access management
• Ideally adopt an approach of least privileged. = As signs just enough privileges to a user to perform their respective duties.
• Consider the following:
  • Restrict admin privileges as far as possible.
  • Use multifactor [at least two to achieve] authentication:
  • Something you know [e.g., password]
  • Something you have [e.g., cryptographic token];
  • Something you are [e.g., biometric].
• Enforce strong passwords, with strong passphrases.
• Enforce frequent password changes
• Do not reuse passwords for multiple accounts.

Cyber security awareness & training
• Implement this ASAP.
• Encourage staff to flag anything out of the ordinary.
• Focus on the high risk areas.
• Various resources online to identify an applicable awareness program

Encrypt sensitive data
• In transit and at rest.
• See Regulatory frameworks on customer data management.
• Take precautions with all types of sensitive data.
• Take special care in managing the encryption keys.

Use network- & host- Firewalls
• Firewalls monitor & filters incoming/ outgoing network traffic based on an organization's security policies.
• Helps safeguards the network from phishing attacks.
• Important for cloud systems.

Anti-virus & anti-malware software
• Install & keep updated on all hosts
• Update virus definition files & application.

Segment your IT network
• This helps to contain an attack in case of compromise.
• Allows you to apply various levels of defence in depth mechanisms to protect critical hardware, software & data.

Glossary

Antivirus Software that detects, stops, and removes viruses & other malicious software.

Cyber attack Malicious cyber attempts to damage, disrupt, or gain unauthorized access to computer systems, networks, or devices.

Cyber security The protection of devices, services, networks & the info on them, from theft or damage.

Data server A computer or program that provides other computers with access to shared files over a network.

Denial of Service [DoS] Legit users are denied access to computer services, usually by overloading the service with requests.

Digital footprint A [footprint] of digital info left by a user's online activity.

Encryption The transformation of data to hide its content.

Firewall Hard/ Software designed to prevent unauthorised access to a computer or network from another.

Hacker Someone who violates computer security for malicious reasons or personal gain.

Hardware Any physical component of a computer system

Malware [malicious software] Software intended to infiltrate & damage or disable computers.

Network firewall Device that controls traffic to & from a network.

Password A secret series of characters used to authenticate a person's identity.

Patching Applying updates to hard/software to improve security &/or enhance functionality

Personal firewall Software on a PC that controls network traffic to & from that computer.

Personal information Personal data relating to an identifiable living individual.

Phishing Crime where criminals try to obtain confidential information [including user names & passwords] from users. Usually done by email, which appears to have been sent by a legit organization. The email usually contains a link to a fake website

Ransomware Malicious software that renders data or systems inoperable until the victim pays a ransom.

Risk Something that could prevent an organization from meeting 1 of its goals.

Risk assessment The process of identifying, analysing & evaluating risk.

Router Device that directs messages within or between networks.

Server Computer that provides data or services to other computers over a network.

Software The programs & other operating info used by a computer.

Threat Something that could cause harm to a system or organization.

Two-factor [multi-factor] authentication. The use of 2 different components to verify a user's identity.

Username The short name, associated with a particular computer user.

Virtual private network [VPN] Link[s] between computers or local networks across different locations using a wide area network that cannot be accessed by other users of the wide area network.

Virus Malware loaded onto a computer & then run without the user's knowledge or knowledge of its full effects.

Vulnerability A flaw or weakness that can be used to attack a system or organization.

Worm Malware that replicates itself so it can spread to infiltrate other computers.