VALTUS

Cybersecurity

Addressing the human factor

Addressing the human factor in cybersecurity

In these times of uncertainty, if you ask your Board of Directors what the greatest risk for your business is, you will most likely hear: “cybersecurity” (cyber incidents identified as top global business risk in the 2022 Allianz Risk Barometer[1]). In 2021, the UK was the 3rd country most affected by ransomware[2].

Many information technology players would dream of being noticed by managers and shareholders of companies that shape the economy. It is clear that cybersecurity concerns are shared in a heterogeneous way by employees and businesses: less than half of organizations have implemented at-scale cyber awareness training programs[3].

The fact is, cyber risk is not merely about technology, it is above all related to people and the different teams working with companies. Hackers play with this, using quite unsophisticated hacking techniques such as email spoofing (forged email sender addresses), phishing (sending infected attachments or malicious links) and flaws linked to a machine configuration and software obsolescence. Often lurking in poorly monitored technical spaces, hackers study their targets before moving on to the actual attack... and this attack does not necessarily come with a ransom note.

Once the moment of shock is over, companies have a fairly limited range of responses to find their way out of the crisis, then strengthen the protection of their systems in the broad sense without of course forgetting awareness-raising of all stakeholders... The question is no longer whether a company will be attacked but whether it will be able to respond when it is.

Thus, the NIST cybersecurity framework[4] facilitates the implementation of a virtuous circle of operation within organizations: identify, protect, detect, respond, recover.

Ways to prevent cyberattacks

Ahead of an attack, the most resilient companies plan and get ready. Here is where technology plays a critical role. Publishers, manufacturers, and start-ups in the sector are offering solutions commensurate with the growing sophistication of attacks. These quickly become a puzzle with gaps also requiring the creation of a responsive scheme, based on people and procedures:

- Establish an active watch and prepare, bearing European recommendations in mind (https://www.enisa.europa.eu/).
- Train and raise awareness among employees, service providers and partner companies: knowing how to recognize phishing, getting organized when facing CEO fraud attempts or the dissemination of fraudulent bank details to customers, refusing connected gifts or USB flash drives carrying potential malware (malicious software, viruses)…
- Simulate cyber-attacks and evaluate company responses, just like those companies who regularly conduct fire drills.
- Take out cyber insurance, which also requires set up of proven IT security systems.
- Encrypt personal and sensitive data so it is not blackmailed on the Dark Web[5].
- Make regular backups, store them outside the corporate network, and regularly test the recoverability of these backups.
- Build and – above all – test a DRP or “Disaster Recovery Plan” in order to proceed with asset recovery as quickly and as accurately as possible.
- Finally, have a Multi-Factor Authentication (MFA) solution, requiring a user to identify himself through at least two different company-owned devices (PC, tablet, smartphone etc.).

Responding to the computer attack

During the attack, companies who were able to carry out these key initiatives are better prepared. Nevertheless, the crisis management itself requires the involvement of both the company's top executives and of a strategic crisis unit. Specialized firms can help strengthen the crisis communication scheme or aid in the identification of:

- The type of cyber-attack,
- The attacker's motive and origin,
- Patient 0 (who was infected first or the attacker's entry point),
- The size of the breach in information systems,
- Possible data theft or malware injection for espionage, encryption or computer takeover purposes.

Recovery involves restoring data, sometimes the network, computers and often the company directory. The idea is of going back - before the cyber intrusion - to a moment were protecting oneself from the effects of malware is possible. This step is tricky and can lead to loss of information.

What about the ransom, if demanded? Paying to recover data is an "easy" way out with often dangerous consequences. Depending on the origin of the attack, a company may come across a group of experienced cyber-criminals whose "ethics" consist effectively in activating its threats (posting/selling of sensitive data on the Dark Web) and keeping its promises (returning data over ransom payment).
However, anyone who pays a ransom will undoubtedly be spotted by other groups and exposure to further costly attacks will only increase. Some cyber insurance plans provide ransom repayments depending on the country where the attack takes place, and its local regulation. This is a sensitive regulatory topic, subject to frequent shifting. For example, back in 2017, there was a Russian ransomware attack on Ukraine called 'Not Petya' that nearly took out 2 global companies, Maersk, the Danish shipping company, and Merck, the American pharma. Merck claimed on their insurance. The insurance company said it was a nation state attack and therefore an act of war and was not covered. Merck took them to court and eventually won earlier this year. It cost the insurance industry $1.4bn. As a result of the Merck case, Lloyds of London have regulated that as from 31 March 2023 nation state attacks are not to be covered in insurance policies. USA insurance companies are also doing the same.
If the decision not to pay the ransom can be terrible for the immediate survival of a company, it is the best option for its medium and long-term sustainability.

After the storm

Once the crisis is over, organizations are especially required to strengthen their technical systems (VPN, firewall, antivirus, email filtering, etc.). Regular checks through IT security audits allow better understanding of vulnerabilities. Companies initiate or speed up projects that improve the security of information systems:

- Security governance committees bringing together stakeholders meeting on a regular basis and chaired by the IT security manager and a sponsor, such as the company's General Secretary,
- Annual organization of cyber-crisis management exercises,
- Comprehensive and up-to-date inventory of hardware and software produced using a CMDB (configuration management database),
- Reduction of technical debt (exit of outdated technical solutions no longer supported by publishers),
- Anticipation of threats through regular monitoring of the techniques used.

Outsourcing the monitoring of the information system can be an adequate solution (using a “SOC”: Security Operations Center) if the company is able to process the various alerts that the SOC will send out.

This overview of the possible schemes or devices shows how cyber risk is both a technical matter – like everything related to business information systems – and an organizational matter whose human dimension is the key success factor to building a robust system to prevent and deal with cyber-attacks.

In times of crisis, a seasoned IT security manager must have the right habits, the right persuasive language within the company, and the right network of partners. It is exceedingly rare to have an IT security manager who is both a firefighter and a talented architect of a fortress-style system.

This other architect role calls for project management, pedagogical, anticipation, and technology watch abilities. Interim management is an innovative approach adopted by a growing number of companies occasionally seeking a manager with these two skills or wishing to complete the skills of an in-house IT security manager. As interim managers adjust quickly and are result-orientated, they have what it takes to deal with urgent cybersecurity issues.

[1] Allianz Risk Barometer, January 2022
[2] 2022 NordLocker Report
[3] PwC 2022 Global Digital Trust Survey
[4] https://www.nist.gov/cyberframework
[5] Hidden set of websites that can only be accessed by a purpose-built browser such as TOR
[6] https://atlasvpn.com/blog/31-of-us-companies-close-down-after-falling-victim-to-ransomware