OUR GUIDE TO

CYBERSECURITY

yellowcube

updated on 07/21/23

LET'S UNDERSTAND

CYBERSECURITY

yellowcube

THE ELEMENTS OF CYBERSECURITY

yellowcube

People, process & technology

Real cybersecurity can only be achieved by continuously operating business-optimized **processes**, that are based on ideal **technologies** best utilizing the organization's available **human resources**.

For example, this is why we can never achieve real security at home. Even while deploying the best technologies with very simple processes to protect a family wifi, still there won't be anyone to operate and upkeep cybersecurity.

So in this scenario, we are limiting ourselves to automatic protection against simple attacks, and we cannot keep up with evolving threats.

Self-improving security process

The core of cybersecurity is an always evolving process that follows the advancement of both cyber threats and protection technologies.

First, we **prepare**: based on perceived business risks and threats, we create our security model. Then we deploy our **preventive** cybersecurity measures, which will immediately block known threats. As we expect prevention to be imperfect, we prepare to **detect** threat actors bypassing prevention. Then we **respond** in time to stop the attack before damage is done.

Finally we draw the right conclusions and update our cybersecurity model to avoid and make similar attacks in the future impossible.

THE 3 PILLARS OF CYBERSECURITY

In the decades of cybersecurity evolution, three major pillars were created to support different security aspects.

First **preventive security**, like anti-virus engines and firewalls were made to automatically stop threats, without human intervention.

Later the emphasis moved to **detection and response** to stop threat actors bypassing our preventive cybersecurity measures.

In the meantime, best practices and secure business processes are implemented by **cyber hygiene** solutions. For example, passwords on post-it notes are replaced by password safes or data leaks are being handled by DLP solutions.

yellowcube

Just like our own health

To understand cybersecurity better, we could compare it to the upkeep of human health.

Prevention utilizing vaccines simply protects against known diseases. But when we have no vaccine yet against a new virus, just like with Covid-19, the whole world stops for months.

Detection and response is just like continuous health checkups: we utilize advanced technologies like MRI, artificial intelligence to detect yet unknown threats. If we do it well, we won't even know what could have developed from it, as we don't wait around for years to see what happens.

Finally, if somebody is still challenged by bad personal hygiene, their priority should be to improve on that before turning to other pillars.

Prevention

Using continuously updated threat databases, prevention immediately stops know threats.

Detection and response

Detects attackers that successfully bypass prevention and provides fast response capabilities to lock them out before they would be able to reach their goals or do any damage.

Cyber hygiene

Resolves toxic situations and manages internal risks rooted in either unintentional carelessness or intention to do harm by the organization's own employees.

LET'S BUST

CYBERSECURITY MYTHS

yellowcube

CYBERSECURITY MYTHS

yellowcube

„Defense is disadvantaged”

It is a common myth to think that attackers would have more resources: any criminal group must have **less time and money to spend** on a single attack, then the cybersecurity resources of a prepared organization defending against it.

Although it is true that the attacker needs just one opportunity to get inside a network, but it has to be very difficult to carry out a complete attack chain and remain undiscovered for weeks.

Protecting our own networks, just like protecting our own warehouses against burglars **can never be disadvantaged** if we prepare and maintain our lines of defenses well.

„Preparing for the unknown”

An often returning deflection of responsibility is to constantly prepare for the unknown. Although we still **haven’t seen any real unknowns**, which couldn’t be resolved by proper understanding.

For example, a **zero-day vulnerability** is not an unknown, just statistics: if we know, that our source code contains on average one exploitable bug in 10.000 lines, then we can calculate the number of zero days in it. Then it is our responsibility to prepare for them being exploited.

However, **a real unknown** could be when a burglar breaks in by demolishing a wall: this completely invalidates our security model and we need to rethink it from the beginning.

„Security is made by products”

We already busted our last myth earlier: no single product will provide security without the right business process and people operating it.

What’s more, a large scale research* showed that **one third of all security vulnerabilities are found in the security software itself.**

There is no point in purchasing many security products without proper oversight, as we are probably just making our network more vulnerable and exploitable. Instead, we should operate an optimal size, maintained cybersecurity stack.

* Source: Mudge/Google, auditing over 20 000+ enterprise networks, 2022-2023

MINIMAL

CYBERSECURITY

yellowcube

MINIMAL CYBERSECURITY

yellowcube

In 2023, it is not trivial to just start with cybersecurity and **catch up on decades** of it's evolution. Although by learning from others' mistakes we can define a minimal and efficient cybersecurity core that can be logically developed in the future.

Essential to understand that **cybersecurity is a core part of business**, so our goals are the same and should be measured similarly. Cybersecurity cannot be limiting for business, and business should not overwrite security aspects.

If we don't keep this in mind the cybersecurity team can quickly become the enemy of business, which certainly leads to pointless conflicts.

Cybersecurity starts with **awareness**. Every decision maker must understand the business risks on their own level and depth, otherwise no budget will be provided to develop cybersecurity.

From a technical aspect security starts with authentication: a **user directory** and equipment inventory, like Active Directory.

Devices are protected by **endpoint security** and patch management to remove all known threats and vulnerabilities, while the **firewall** segments the network into security zones.

Implementing **detection and response** prepares us for a future cyber incident, and **practicing the reaction plan** will complete the minimal security.

Minimal cybersecurity in 2023

0. Leader awareness and visibility of business threats will help allocate the required budget

1. Authentication: user and device directory

2. Removing known vulnerabilities with patch management, security posture management and deploying an endpoint security solution

3. Network segmentation with firewalls

4. An implementation of **detection and response**

5. A practiced **Incident reaction plan**

And later we can deploy the best business specific defenses: multi-factor authentication, advanced phishing and email security, etc.

HOW DEVELOPED IS OUR
CYBERSECURITY?

yellowcube

LET'S MEASURE CYBERSECURITY.

yellowcube

We can start with the **simplest audit on paper**, by summarizing our lines of defenses based on the amount of resources needed to maintain, versus to bypass them.

Logically our security should be based on defenses that are **cheap to maintain, while costly for the attacker to bypass**. Otherwise we should disband that defense and use those resources better.

For example, deploying Network Detection and Response is easy, while it makes the attacker's job difficult. However an Endpoint Detection and Response is significantly more difficult to maintain while it's not harder for the attackers, so in this case an NDR is a better choice then an EDR.

Continuous security validation

For a more comprehensive approach, we can use offensive security products that can objectively measure our cybersecurity with real attacks.

These Continuous Automated Red Teaming (CART) and Breach and Attack Simulation (BAS) solutions will only make sense when our security is prepared and we are **not missing any pillars**.

As we start to **objectively measure** the performance of the entire security stack, we can start to willingly increase the organization's **real-life cyber resilience**, remove now under-performing security products and validate the efficiency of new solutions before deployment.

Continuous security validation with **Cymulate**

CYBERSECURITY MATURITY

yellowcube

After understanding business risks and defense strategies, we can identify our **level of maturity** based on the three pillars of cybersecurity.

Logically all problem-solving starts in an **initial** stage, cybersecurity is no exception here.

As we go deeper and understand the problem better, first we'll try to solve it with ad-hoc **repetitive** tasks, just like fighting fires.

Later on these tasks form a **documented** system, while as we integrate it into the business better, we get to continuously **managed** cybersecurity.

As the business realizes the competitive advantages of operating good cybersecurity, we would achieve the **optimal** state of cybersecurity.

Organization's cybersecurity maturity

initial **Cybersecurity ignorant**	The organization is unaware of its cyber risks. Cyber incidents are either left unknown or acknowledged only after visible damage was done.
repetitive **Improvised cybersecurity**	Ad-hoc cybersecurity products are deployed in silos with no company-wide oversight. Detected incidents are managed manually, like fighting fires.
documented **Leadership decision**	Leadership decision is made either by realization or by suffering a cyber incident. Responsibility and budget is given to a new cybersecurity manager.
managed **Managed cybersecurity**	Continuously managed cybersecurity is implemented with company-wide defenses, incident management and clear directions for development.
optimal **Optimal cybersecurity**	Cybersecurity is validated by real-life attacks to build up the organization's cyber resilience. Threat intel and best practices are shared among peers.

Cybersecurity maturity based on the three pillars

Cybersecurity is based on the three pillars discussed earlier: known and avoidable threats are stopped by **prevention**, while the rest is managed by **detection and response** capabilities. **Cyber hygiene** combines best practices and secure business processes to help employees avoid toxic and risky security conditions.

	First pillar **Prevention**	Second pillar **Detection and response**	Third pillar **Cyber hygiene**
Initial	Built-in and free security products.	Not available.	Not existent.
Repetitive	Siloed, improvised security products.	Manual firefighting and recovery after incidents.	Cybersecurity education.
Documented	Defenses deployed based on specific business risks.	Incident management processes and practiced recovery plan.	Supervision based on business risks and monitoring third-party suppliers.
Managed	Change management and purposeful improvements.	Company-wide threat visibility and managed incident handling.	Incidents are created by risky behavior, employee trainings are automated.
Optimal	Validated cybersecurity with objectively measured efficiency.	Continuously validated capabilities with response automation.	Risk level monitoring of employees predicts and prevents incidents.

yellowcube

Let's translate maturity levels to products

We can better determine the maturity of cybersecurity and possible directions for improvement based on already deployed products and defenses. These don't necessarily build on lower levels, **we can skip already outdated technologies**. These levels can further be clarified based on business-specific risks, with methods like the attacker/defender resource cost comparison discussed earlier.

	First pillar **Prevention**	Second pillar **Detection and response**	Third pillar **Cyber hygiene**
Level 0	Built-in and free security products	Manual recovery from incident damages	No human risk management
Level 1	Endpoint security (antivirus, anti-malware)	Log collection (SIEM)	Multi-factor authentication
Level 2	Patch and security posture management	Incident management system	Management of mutually used passwords and API keys
Level 3	Network segmentation with firewalls	Anomaly detection, behavior analysis (UEBA)	Monitoring privileged users and third parties (PAM)
Level 4	Gateway security, content filtering, web filtering	XDR products with zero-trust security	Securing home office and remote workplaces
Level 5	DNS security	Cloud and email detection and response	Secure internal communication
Level 6	Data classification with formal data access management	Data-centric detection and response	Oversight of data movements
Level 7	Industrial (OT) security	Automatic response with playbooks (SOAR)	User behavior and risk monitoring (UEBA)
Level 8	Cybersecurity validation	Cybersecurity validation	Cybersecurity validation

yellowcube

WHAT MAKES CYBERSECURITY **EFFICIENT?**

yellowcube

EFFICIENT CYBERSECURITY

yellowcube

In two decades of it's operation, through thousands of enterprise and government customers, Yellow Cube learned how to build **efficient** and **sustainable cybersecurity** for the long term.

Turnkey cybersecurity

Our most successful solutions **activate instantly**, making previously unmanaged risks immediately visible and manageable.

With our turnkey approach, **cybersecurity improvements** can be quickly illustrated even through short evaluation periods, to justify the release of budgets required for a final implementation.

Simple product, no maintenance

We believe in utilizing **simpler products to their full extent**, rather than just a small piece of functionality of a complex solution.

A security product ten times more complex probably comes with ten times more vulnerabilities and a wide variety of potential configuration mistakes, making the **real-life security improvement after deployment questionable.**

A simpler solution with no maintenance needs however allows **our time to be better utilized** for building and improving cybersecurity and not being bogged down in complex maintenance.

Artificial intelligence

Yellow Cube has been deploying AI-based solutions since 2014, as soon as it became clear to us that AI is the best and probably only way to **bridge the skill gap** and to add security analysts that are an impossible hire for most companies.

This approach makes our solutions universally usable, even with high fluctuation. Know-how is **not dependent on a single person** and new colleagues can independently pick up the skills.

AI also enables customers to provide **optimal cybersecurity around the clock** with the right automation tools at their fingertips, without expanding the already available workforce.

EFFICIENT CYBERSECURITY

yellowcube

Cost-efficient and local

Customers in our region often work with very **limited budgets**, so we also have to select our vendors with the required flexibility and ability to meet even the tightest budgets.

In two decades of operation, we collected happy customers in all areas of business and government. We always prefer **open consultation** between industry peers and learning from each other, instead of running long proof-of-concept trials and re-iterating evaluation cycles.

Our free workshops and webinars bring all our products within arm's reach to demonstrate the latest cybersecurity capabilities and understand our defense strategies to the fullest.

ABOUT

US

yellowcube

ABOUT US

yellowcube

The Yellow Cube Group

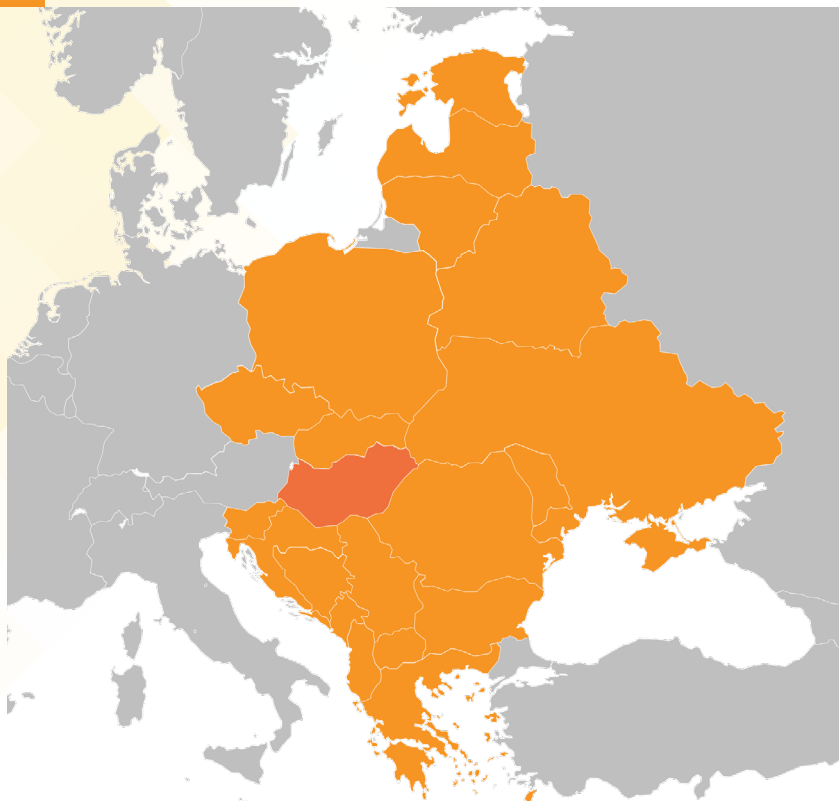
Based in Budapest, the privately-owned Yellow Cube Group brings leading cybersecurity solutions to Central and Eastern Europe.

We believe that every organization is entitled to their own **digital sovereignty** in a world of rising sophistication and amount of digital threats.

That is why our job is to **evangelize, localize and educate** new cyberdefense products that allow the region's relatively small governments and enterprises to efficiently and reliably defend their networks against much more powerful digital threat actors.

Yellow Cube in numbers

- Founded in 2005
- 20 employees
- € 8 million yearly turnover
- 415 active partners
- 757 trained & certified engineers
- **Prevention:** 3992 firewalls & 59,503 hosts
- **Detection and response:** 238,635 hosts
- **Cyber hygiene:** 15,681 users



GET IN TOUCH WITH US

yellowcube

yellowcube.eu

hello@yellowcube.eu

Budapest, Nádorliget utca 7A

facebook.com/YellowCubeCyber

linkedin.com/company/YellowCube