Auteur: Paul W.M. Oor is freelance Security & Data Protection Manager/Consultant. Paul is te bereiken via paul@shared-experiences.nl. Dit artikel is eerder verschenen op de ISACA NL Chapter https://isaca.nl/nieuws/cisos-enabling-business/#_ftn1.

CISO's enabling business

The 10 commandments for CISO's in 2022

In June 2021 ISACA NL allowed me to publish my opinion on what business leaders should do to take ownership for security and enable their CISO's to be more effective: 'CEO's enabling CISO's; the 10 commandments for CEO's when positioning a CISO in their organization...' (1) In this sequel I'll explain my sense of urgency and how we need to change security governance, now presenting: 'The 10 commandments for CISO's in 2022' (2). Adapting our organizations to survive and prosper in an increasingly complex, chaotic world.

The mentioned article triggered discussions with business managers and my security peers. Managers challenged me on them taking full ownership of cybersecurity and data protection while my professional peers saw the chance of a seat in the boardroom vaporize. Both audiences urged me to explain why this change is required now? A hopeful sign! We need all the attention we can get to close the gap between organizational leaders and security professionals, managing expectations on both sides.

Piracy and an increasingly complex world

We live in a time where our activities in the past are re-evaluated and excuses offered. With the vision of hindsight, the activities of my (Dutch) ancestors were often debatable to say the least. A lot of our wealth and fortune originates from piracy (3) when measured by today's standards. In those days however, my ancestors were tolerated and respected in their society. Their activities were considered of vital importance for the nation's prosperity as they were developing global supply chains and colonies by semi-legit activities. Tolerated and supported by governments and large commercial organizations like the VOC (4). Today's developments and threats related to global cyber-supply chains and data colonies have a lot in common with this period of history. Hackers i.e., pirates, force us to collaborate, innovate and drive us to maturity. At the same time, we're in business with the nations and multinational companies who back and protect todays pirates while loot and ransom are still being used to become more powerful.

Taking back control

During several centuries pirate activities proved to an essential driver for the development of the colonies and trade-routes. In the end nations took back control by treaties and navies, protecting legitimate merchant fleets and fortified, controlled cities in the colonies. History seems to repeat itself in cyberspace. Some nations provide protection to today's pirates; hackers are respected, extremely rich and popular. Their comfortable position is now more and more challenged and tensions are rising due to the vital importance of global cyber supply chains and data-colonies. This complex landscape has thus become a topic to be effectively tracked by leadership in all organizations.

Laws and regulations vs. effective cybersecurity

History has shown that protecting interests and sovereignty with legitimacy i.e., laws and regulations has its limitations. Nevertheless China, the USA, Russia, the EU and others are developing stringent laws and regulations to protect their digital sovereignty and data. But on top of that everyone, even the EU (5), is stepping up their defensive and offensive cyber-capabilities. We've come to realize that laws and regulations alone are not effectively protecting our digital interests and sovereignty. Developments in this increasingly complex landscape; compliance combined with effective protection is a topic requiring direct involvement of leadership in any organization too, supported by security and data protection professionals.

Global politics, cyber and business

Organizational leaders must monitor the impact of this fast-moving, unpredictable, war-like landscape. Like the military do: OODA: Observe, Orient, Decide and Act (6). Cybersecurity has become a matter of national security in many countries and has a direct impact on any organizational strategy and operation. With whom can and may your organization conduct business today and in the future? Who's to be trusted, legally and effectively reliable in the long run? Where can and may we process our data, in which data-colony? Business leadership is accountable and responsible; as professionals we must support them. With the emphasis on support, there's no way cybersecurity and data-protection professionals can or will carry all of the burden, no matter how well we are paid. Leadership must integrate cyber in their governance. Business managers have to talk cybersecurity and data-protection if they want to trade supported by professionals like us, as described in the `10 commandments'!

Address complexity: tangible advise for a challenging job

Managers can't maintain their traditional attitude; 'I've hired expensive security professionals and services; let them take on their responsibility and deal with it'. Security must be integrated in the organizational governance and the DNA of the organization. Everyone was well aware of the threats and dealt with it. Commercial companies, state sponsors and everyone in the crew, from captain to deckhand, were always alert and responsive. Protecting their lives, trade and business profits.
Considering an unpredictable future and the evolving threat landscape means that our organizations and we, as professionals, must reach a similar level of vigilance. I hope you will find 'The 10 of commandments for CISO's in 2022' helpful to align with your leadership and support them to effectively integrate security in your organization.

The 10 commandments for CISO's in 2022

1. Take good care of yourself. Like any first responder or person working in high pressure environments; ensure good physical and mental health. Only when you are safe and in good shape, you can be of service and support others.
2. Don't ask for a security budget. Security is the responsibility of the entire organization, not of a single department. Adequate funding and related cybersecurity-KPI's (7) should be requested by and allocated to divisions and departments. I've never understood the bill of materials of security costs as referred to in surveys or demanded by financial controllers. The salary and expenses of the CISO and perhaps some very specific services exempted. The majority of security costs and investments are tactical and operational costs, to ensure business continuity of the whole organization. You don't specify costs for brakes, mirrors and seatbelts in a car as optional security cost, do you?
3. Forget about 100% security assurance. Some colleagues are struggling in their organization and even considering employment elsewhere as they consider the organization's efforts not in line with their professional standards. As a CISO you must accept to live with uncertainties and risk acceptance by management. Which is alright, as long as you provide tangible, pragmatic professional advice and risks are seriously evaluated and explicitly accepted, not ignored. Embrace risks, changes and innovation without becoming reckless.
4. Develop and maintain an excellent information position. Invest heavily in your professional network to maintain situational awareness and keep abreast of developments relevant for your organization. Not limited to technology! Global politics and compliance developments (8) included! Try to recognize and be aware of plans within plans, schemes within schemes in the landscape to identify relevant developments and support your organization to address potential risks.
5. Invest in continuous education. Our profession requires at least a basic level of knowledge in many areas and this knowledge must be maintained, despite rigorous changes. Security certification helps as it provides at least a Common Body of Knowledge (CBK) (9) and will get you recognized for your professional drive and – at least – basic knowledge and capabilities.
6. Track environmental and social developments. Security and data protection are increasingly important for organizations as they must live up to the changing expectations and standards in society. Not limited to formal compliance; be aware of what's socially, politically and ethically acceptable now. Tracking e.g., politics is essential in our job to advice e.g., in which data-colonies (clouds) your organization's data can be processed, today and in the long run!
7. Declassify data and information. Reconsider need-to-know to increase resilience and vigilance of your organization. Make information more widely available within your organization. Declassification information where possible; enabling Teams of Teams (10) in today's dynamic environment. Only a very small amount of data in the organization really needs strict protection; focusing on the protection of these Crown Jewels will reduce workload and costs.
8. Stop fighting for a CISO-seat in The Board. It's a distraction and waste of your precious time and energy. Focus on having one or more board members becoming aware and familiar with your security agenda. Support these sponsors in the board to get security implemented, financed and controlled in the whole organization. Get them as interested in security KPI's as they are in the financial performance of the organization.
9. Forget about compliance, rules and regulations. OK, that sounds a bit harsh but DO focus on effectiveness; no pirate-hacker will be scared away by laws or security certification. On the other hand, don't ignore developments on standards, laws and regulations. Get and stay familiar with these and treat potential non-compliance as a potential, serious threat to the organization.
10. Focus on organizational readiness. Avoid becoming too complacent and too dependent on structures and processes. Hackers and their sponsors are unpredictable; make sure your organization is prepared for the unexpected; simulate and exercise. Think evil and out-of-the-box. Always supplement PENetration tests with frequent Red/Blue Team exercises. Practice will make everyone in the organization better understand what's at risk. By doing so your organization will be in a strong position when an inevitable incident occurs. During an actual situation stress will be higher because it's real. But nothing will be totally new!

Can we still learn from the past?

The world has become more complicated, but the real challenge is its complexity. I've lost my 'been there, seen that, done that' attitude. Experience counts but even seasoned business managers and security professionals must admit that experience is not enough anymore. It has to be complemented with a new attitude, genuine interest in developments in many areas and the input of the new generation in our organization. Leading us to increased organizational vigilance and commitment of leadership on security to ensure organizational resilience.

There is some comfort in the parallels with Piracy in the old days. Dealing with continuous piracy by Japanese pirates raiding the coasts of China and Korea in medieval times rulers realized that piracy was something to be considered as something natural that could not be avoided but had to be reacted on. Deal with it, even make use of it. This resulted in a kind of equilibrium, a balance, formalized by a treaty (11). Compromising with, even pardoning and hiring pirates and at the same time disrupting their business cases. By challenging sovereignty and ceasing ground and other possessions of rulers in areas where pirates were sheltering and protected.

Today's piracy is complex but applying this approach today might be effective again. It's still all about wealth, power, controlling supply chains and sovereignty. I'm embracing tomorrow with optimism, confident that our security community, working with management can deal with today's threats and challenges. As long as we adapt our modus operandi to cope with a dynamic and complex world. Like in the days of global exploration by seafaring nations we're going through a fascinating period of change, only quite a bit faster than our ancestors… This makes security a great and challenging job never a dull day!

ISACA Netherlands Chapter

References

(1) https://isaca.nl/opinieartikel/ceos-enabling-cisos/

(2) I'll be using the term security instead of security and data protection to improve readability. However, I strongly believe in close collaboration and merging activities of CISO's and DPO's! Especially since too many DPO's focus on the legal aspects of data protection while effective protection of (personal) data has to be taken care of as well.

(3) https://en.wikipedia.org/wiki/Golden_Age_of_Piracy

(4) https://en.wikipedia.org/wiki/Dutch_East_India_Company

(5) https://www.consilium.europa.eu/en/policies/cybersecurity/#

(6) John Boyd, Military Strategist

(7) Key Performance Indicators

(8) Advancing IT, Audit, Governance, Risk, Privacy & Cybersecurity | ISACA

(9) (ISC)² CBK | Common Body of Knowledge (isc2.org)

(10)Team Of Teams: An Emerging Organizational Model (forbes.com)

(11) Wokou, Wikipedia