How to use cybersecurity as competitive advantage

by  **Tomáš Hettych**, Senior Manager Cybersecurity, Risk Assurance Services, PwC

These days, you can read about information security a.k.a. cybersecurity almost every day in the media. The cybersecurity topic is often simplified to hackers' attacks and fines for non-compliance with GDPR. But this view is far from reality. Three years ago, the total amount of damage related to cybersecurity already exceeded damage from all other security areas. Today's bad guys do not rob banks with masks and guns, they use their computers to strike.

Information security vs. cybersecurity
Let's start with some terminology and clarification of terms. Cybersecurity is a subgroup of information security related to cyberspace. In other words, information security deals with information in any form and cybersecurity only deals with information in digital form. Together with business continuity and physical security, information security adds up to a bigger domain: risk management. And today, cybersecurity is the new, "sexy" term for anything related to information security and IT risk.

New cybersecurity legislation
Why do we read about cybersecurity almost every day? The first reason is that there are new cases every day: new sophisticated attacks, new malware, and new fines for non-compliance.

The second reason is new legislation: the General Data Protection Regulation (GDPR) adopted on May 25th 2016 and the NIS Directive (Cyber Act) on July 6th 2016. Both acts highlighted the need for information protection at every organization and the setting of general rules for assessing and managing risks.

Cybersecurity and its relationship to GDPR
GDPR is an intimidating issue due to huge fines and its very general approach. Because of the very general language used in GDPR, full compliance is almost "mission impossible".

Some regulators imposed very high fines with very strange explanations and affected organizations appealed to the courts. That is why companies are empowering lawyers or compliance officers to deal with GDPR.

> **Because of the very general language used in GDPR, full compliance is almost "mission impossible".**

On the other hand, the Cyber Act is more specific and based on industry best practice and standards. Therefore, it is much easier for organizations to follow its regulatory requirements. The usual owners of the topics are chief information security officers (CISO) and chief information officers (CIO).

What is the connection between GDPR and the Cyber Act? Data protection and information security are overlapping topics and could not exist separately and both acts force organizations to implement new technical and organizational measures.

Usual positioning of cybersecurity at companies
A few years ago, most organizations (except for banks, insurance companies and telco operators) had little in the way of information security. Even if they did, they usually placed security in the IT department or facility management. The usual approach underestimated the information security domain. A similar trend was visible 10-15 years ago in the IT sector.

Fortunately, today's approach is dramatically different, and hardly any organization underestimates the management of cybersecurity and IT. The main reasons are given above: malware, hackers, fines and the increased complexity of information systems. Most organizations have created new departments of information security or risk management and are finally treating the topic as extremely important.

Conclusion: why not spend more on cybersecurity and use it as a competitive advantage?
Cybersecurity is no longer just a cost with no benefit and information security functions are not just cost centers anymore. Implementation and cybersecurity management is a complex project which involves many business units. Some important advantages are:

- Prevention of data leaks and malware
- Intrusion detection and prevention
- Protection of intellectual property and company image
- Saving company assets

Managing cybersecurity can help organizations achieve their business goals and fulfil their strategies. Almost all organizations are now dependent on information systems which require a proper level of protection of information assets. This correct and proven level can be evaluated and assessed through various industry standards and certificates, which will set apart your organization from others at a time of tough competition.

So what are the dangers of not paying attention to cybersecurity? Here are some examples: a five billion dollar fine for Facebook in 2019 for privacy issues, the worldwide WannaCry virus attack in 2017, one billion accounts comprised at Yahoo in 2013, and the Stuxnet attack on Iran's nuclear program. It can mean: losing your business, losing your clients' data, and huge fines.