# CYBER SECURITY

# TOP TEN TRENDS AND KEY RECOMMENDATIONS FOR 2019

# TOP 10 CYBER SECURITY TRENDS OF 2018

**1. Blurring of Cyber Threat Actors**
Law enforcement and intelligence agencies are all reporting the increased collaboration between nation-state cyber-attack groups and organized criminal cyber-attack groups worldwide, especially in China, Russia, Iran, and North Korea.

**2. Rise of Business Email Compromise (BEC) Attacks**
Rapid growth of social engineering based cyber spoofing attacks on companies globally, typically focused on the payment of invoices to wrongful suppliers.

**3. Growth of Spear-Phishing Email Attacks**
Increased number of spear-phishing attacks targeting senior company executives especially CEOs, CFOs, and Controllers for unauthorized electronic transfer of funds.

**4. Expansion of Ransomware Attacks**
Over the past year there has been a 350% increase in the number of ransomware attacks globally, with an ever increasing focus on the healthcare industry.

**5. Exploitation of Supply Chain Network based Cyber Attacks**
Significant increase in the number of cyber data breaches resulting from initial unauthorized access via third-party vendors network connections to prime contractors.

**6. Recognition that Regulatory Compliance with Cyber Security Industry Standards Does Not Ensure Real Data Security**
Many companies who have invested in ensuring compliance with various industry standards for cyber security (i.e. PCI-DSS, HIPAA, ISO 27001, etc.) have experienced cyber data breaches. Thus, realizing that regulatory compliance with general information security requirements does not guarantee a company will not suffer a major cyber data breach.

**7. Higher Cost of Cyber Data Breaches = Higher Cyber Liability Insurance Premiums**
As the average cost of a cyber data breach has increased every year for the past five years, so has the average cost of cyber liability insurance premiums.

**8. Increasingly Complex Cyber Security Regulatory Landscape**
The regulatory landscape is often lagging behind and this is especially true in the cyber security area which is by nature characterized by volatility and a high pace of technological innovations. Cyber security related legislature is highly complex and takes place at different levels: national as well as international without proper harmonization on a global level. Therefore it is crucial that companies today anticipate tomorrow‘s regulatory environment.

**9. Shortage of Experienced Cyber Security Professionals**
There is a global shortage of experienced, trained, and certified cyber security professionals to meet the ever increasing demand for cyber security advisory services and managed security services worldwide.

**10. Cyber Attack Fatigue/Burn-out is Affecting Cyber Security Investments**
As a result of continuous news reports of massive cyber-attacks and data breaches internationally, more and more companies are becoming increasingly apathetic to the potential impact on their respective company, often assuming merely purchasing more cyber liability insurance is sufficient, rather than investing in trying to prevent an attack.

# KEY CYBER SECURITY RECOMMENDATIONS FOR 2019

**1. Conduct Email Threat Assessments**
Given the increasing number of cyberattacks via email systems, companies are increasingly looking to conduct periodic email threat assessments, especially to detect malware that made it through their anti-virus software and firewalls which have previously gone undetected.

**2. Perform Network & Endpoint Threat Assessments**
With the expansion of information systems, software applications, bring your own devices, and Internet of Things (IoT), organizations are increasingly testing their network and endpoints via threat assessments using sophisticated Intrusion Detection Systems (IDS) to reduce potential vulnerabilities to cyber-attacks.

**3. Conduct Spear-Phishing Campaigns**
Due to the significant increase in spear-phishing attacks, organizations should periodically test the cyber awareness and susceptibility of their employees to cyber-attacks via engaging certified ethical hackers who can conduct social engineering-based spear-phishing exercises.

**4. Perform Vulnerability Assessments & Penetration Testing**
Most organizations either internally conduct or hire an independent firm to perform some form of vulnerability assessments, via computer malware scanning software, and penetration testing to discover potential external vulnerabilities to cyber-attacks. It is important to conduct these tests at least once a year but, twice or quarterly is better given the constant evolution of cyber-attacks.

**5. Implement Effective and Timely Software Patch Management Program**
The most significant cyber data breaches in the past two years all resulted from organizations not implementing an effective and timely software patch management program of Microsoft and Cisco software.

**6. Establish a Cyber Security Awareness/ Education Program**
The cost effective means to improve cyber security is to create a human firewall by providing quality cyber security educational programs for all of your employees from the top of the company to the bottom.

**7. Conduct Cyber Security Risk Assessments**
It is important to independently verify that an organization's cyber security policies, plans, and procedures are sufficient to adequately protect the organization's digital assets and to ensure regulatory compliance with the appropriate industry cyber security standards.

**8. Implement an Incident Response (IR) Program**
It is critical that every organization has a well thought through and periodically tested incident response (IR) program, including: policies, plan, process, procedures, standard forms, and periodic exercises and/or simulations.

**9. Ensure Continuous Monitoring, Detection, & Response (MDR)**
Every organization should invest in an appropriate level of MDR services based upon the cyber threats their organization encounters or anticipates. The key is to rapidly detect intrusions to quickly contain and eradicate the malware to reduce negative impacts upon the information system and data assets.

**10. Invest in Business Continuity Planning/ Disaster Recovery to Ensure Resilience**
Given the high probability of a cyber data breach, it is essential to have a reliable and secure off-line data back-up system to ensure minimal impact to the organization's operational performance, and protection of the most valuable digital assets from loss or damage.

## SUMMARY

How BDO can help you

Finger on the pulse - As independent consultants, we evaluate your existing environment taking into account the specific context of your company.

We perform a mapping of your strengths and weaknesses in a structured way, and using easy to understand language so that you have a good idea of the existing risks.

First things first - Our approach is gradual, first we make sure that the biggest vulnerabilities in the existing security are addressed. Only when a solid foundation has been laid do we go a step further with the definition of additional checks.

Sounding board - It is not easy for non-technical people to gain insights into actual cyber risks. In our role as independent experts, we are a sounding board for management and make sure that you continue to see the forest through the trees.

Cyber Darwinism - While evolutions used to be rather slow, in today's world the pace is frantic. However, the starting point remains the same: only those who can adapt shall survive. We will gladly guide you in the making of the right choices in your cyber evolution.

## CONTACT

**STEVEN CAUWENBERGHS**
partner
Risk Advisory Services

**E-mail :** steven.cauwenberghs@bdo.be
**Tel :** +32 497 05 12 23

**FRANCIS OOSTVOGELS**
manager
Risk Advisory Services

**E-mail :** francis.oostvogels@bdo.be
**Tel :** +32 474 92 08 00

**NICK HUYSMANS**
supervisor
Risk Advisory Services

**E-mail :** nick.huysmans@bdo.be
**Tel :** +32 486 31 90 45

BDO is the brand name for BDO SCRL/CVBA, a company under Belgian law in the form of cooperative company with limited liability, member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.be.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

© 2018 BDO Services SCRL/CVBA. All rights reserved.