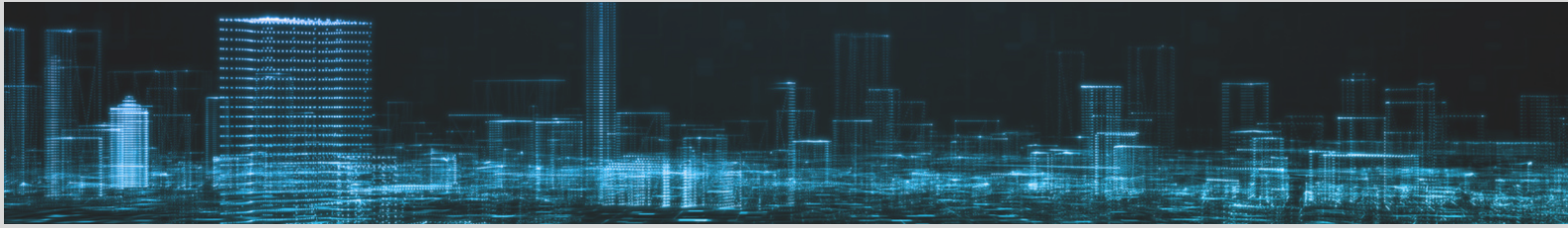


ISACA Belgium Chapter

Institute of Internal Auditors Belgium

ifaci institut français de l'audit et du contrôle internes

Impact paper – The conflict in Ukraine: What do you need to know about cybersecurity?

The conflict in Ukraine requires greater vigilance in cyber security. ISACA Belgium, the Institute of Internal Auditors Belgium and the Institut Français de l'Audit et du Contrôle Internes (IFACI) decided to issue a short impact briefing for all members.

Introduction & Context

Although it remains silent about concrete actions and attacks, clear indications show in the wake of the Ukrainian conflict an expansion of malicious cyber activity, both inside and outside the conflict area. In a digital world, cyber attacks can have a huge impact on daily operations and business, rendering our private and public companies and organizations more vulnerable. Therefore, they need to prepare proactively a mitigation of the potential impact of such events.

This paper intends to raise awareness and to encourage organizations to reflect on their cyber readiness in the context of the conflict in Ukraine. This changing environment calls for a reassessment of the current cyber risk exposure and an evaluation of the need to implement additional measures. Whether or not cyber risk was considered in the past, the current situation may provide an opportunity to assess what needs to be done or to review the existing measures.

What is specific to the Ukrainian crisis context?

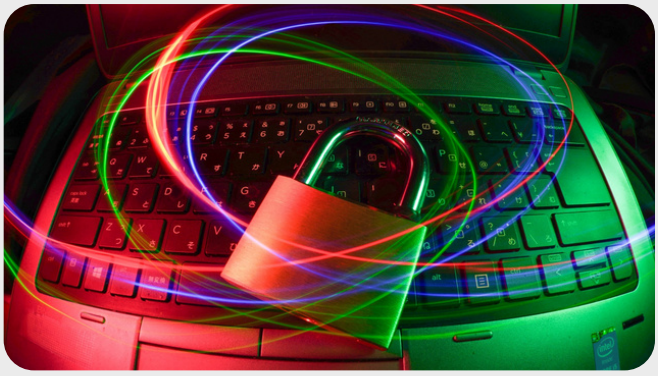
As a result of the sanctions adopted by the European Union against Russia, some sectors such as governmental institutions, financial institutions and energy companies may face retaliation. Since the start of the conflict, the major reported attacks are related to:

- Distributed denial of service (DDoS) attacks focusing on governmental sites and critical infrastructure;
- Attempts to break into e-mail account with targeted spear phishing campaigns;
- Access to systems through exploitation of default Multi Factor Authentication protocols, known vulnerabilities and misconfigured accounts;
- Collection of credentials via brute force attacks to guess the password;
- Data stealer malware such as Formbook;

Wiper attacks (such as WhisperGate, CaddyWiper and DoubleZero) destroy data and render information systems inoperable, sometimes preceded by data exfiltration.

Several Ukrainian IT firms are among the top 100 outsourcers. These companies using information technology services from Ukraine could be directly impacted by the consequences of the conflict. In addition, the organizations could be collateral victims of cyberattacks on networks and infrastructures or malwares.

Role of the Second line of defense



In our view, second liners should :

Value the assets at risks by assessing the effect of impact scenarios:

- confidentiality e.g., intellectual property, critical system configurations;
- sensitivity of personal data e.g., credit card information; health records;
- integrity e.g., compromised business information;
- unavailability of essential information systems.

Perform adversary assessment:

- Identification of cybersecurity adversaries e.g., script kiddies, hacktivists, cyber terrorists and hacker groups, cybercriminals, nation states;
- Interest assessment by determining their level of willingness to commit a threat on a specific asset;
- Power evaluation by estimating their capability to perform a threat successfully

Preventive Awareness

Awareness is an essential element in the control of cybersecurity related risks. Whether in smaller companies and organizations that might not benefit from strong information security capabilities or in larger ones who have invested heavily in technical solutions to protect their crown jewels, the attackers' entry point is often the "human" factor.

Second liners should ensure all internal and external staff are fully aware of the main threats and how to respond to them. Control measures should check the regular performance of trainings and communication actions, but also test their effectiveness (through simulated phishing campaigns for instance). They could also understand the extent to which the awareness plans cover profiles that are especially targeted, such as administrators, VIP staff, finance… handling sensitive information.

Controls should also check how well the awareness of third parties is ensured, as many security incidents over the past years have originated from third parties (e.g., suppliers, clients, IT services providers, business partners).

Therefore the organisation should consider the following:

- How do they keep informed of the evolution of threats and measure their impacts on the organization?
- Is there a regularly updated and clear identification of business-critical and sensitive applications and information assets?
- Are there actions in place enabling to assess:
  - the security of network, devices, applications, web sites (automatic vulnerability scans, penetration tests, configuration reviews….) ?
  - the detection capabilities (such as Red Team tests for instance) ?
  - the crisis management and recovery capabilities (back-up and restore, cyber crisis and disaster recovery simulations) ?

The current conflict in Ukraine is a wake-up call for all of us on the matter of information security dealing with unexpected, unstable events/issues with an unknown duration.

Companies need to proactively adopt a data driven risk-based decision making when implementing risk management, including every phase of the risk management process.

All possible significant vulnerabilities and threats should be developed into risk scenarios and assessed in their application to the organization's particular situation.

Risk scenarios, along with what-ifs, provide a starting point for risk identification and analysis.

As risks could present as different things on various levels of the organization, senior management should be involved in setting direction of the organization and help prioritize of what is important to the business and stakeholders in the organization. For instance, people who are operationally delivering services and products for your organization know what could potentially go wrong, as well as people working in information technology and information security and audit. They can help you understand if you should be involved. Remember that risk is about anticipating what might materialize even if it hasn't happened yet.

What are detection capabilities needs?

Threats and vulnerabilities are present 24/7, even when the organization is not actively pursuing its goals externally or internally. In order to anticipate and identify your own external risk, businesses should have eyes on the news, threat intelligence and security alerts. Most risks are well-known through CVEs (Common Vulnerabilities and Exposures), CERT-EU and numerous commercial resources and threat reports.

From an internal perspective, continuous monitoring of network and system defenses promotes timely detection of threat events and can reduce or eliminate the consequences. Also, by knowing your information technology capabilities, you can:

- Utilize intrusion detection systems to identify potential attacks on the network;
- Detect abnormal events occurring in active security systems;
- Closely inspect the environmental activities to identify deviations in a timely manner.

Depending on the size of your organization, a Security Operation Center (SOC) can help to improve your security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

Here are some key insights to enhance your detections capabilities:

- Ensure that anomalous activity is detected, and the potential impact of events is understood;
- Maintain and test detection processes and procedures to ensure recognition of anomalous events;
- Monitor information system and assets to identify cyber security events and verify the effectiveness of protective measures, e.g., by ensuring vulnerability scans are performed.

What are the required response capabilities?

Effective incident management ensures that incidents are detected, recorded and managed to limit impacts. Incident response activities may be related to broader activities for business continuity and disaster recovery. Incident response encompasses of the operational capabilities of incident management.

The major response steps are:

1. Detection and analysis: identify what happened and how it affects the operations;
2. Containment: contain the breach so it doesn't spread and cause further damage to your business;
3. Resolution: eliminate the root cause of the breach;
4. Recovery: restore the affected systems to get business up and running again;
5. Review: draw the lessons learned to strengthen your organization against future attacks.

Some key questions to measure your own response plan:

- Is your response to processes and procedures executed and maintained to ensure outcomes are tracked to detect cyber security incidents?
- Are your response activities coordinated with internal and external stakeholders, e.g., external support from law enforcement agencies such as CERT…?
- Do you conduct analysis to ensure effective response and support recovery activities?
- Are your organizational response activities improved by incorporating lessons learned from current and previous detection/response activities?

Business Continuity & Disaster recovery related questions:

- Are your recovery processes and procedures executed and maintained to ensure the recovery of systems or assets impacted by cyber security incidents?
- Are your recovery activities coordinated with internal and external parties, e.g., coordination centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors ?

Cybersecurity liability insurance

Cyber insurance policies help cover the financial losses that result from cyber events and incidents. The costs associated with remedial action, including payment for the legal assistance, investigators, crisis communicators, and customer credits or refunds should be covered. The insurance can help recuperate losses related to cyber extortion. Hiring IT forensics experts will often be helpful in recovering compromised data.

What is the role of Internal Audit ?

The cyber threat has been constantly increasing in the past years, and cyber risk has been continuously in the top risks identified by Chief Audit Executives for the past years (Cf. Risk in focus). The conflict in Ukraine is one additional factor suggesting that Internal Audit needs to make sure their organization fully understands where they stand in terms of control of cyber risks, and Internal Audit should play a key role in assessing and identifying opportunities to strengthen enterprise security and resilience.

Ensuring audit plans relevance

Internal audit has a duty to inform the audit committee and the board of directors that mitigating controls are in place and working properly. In terms of cybersecurity, the current situation in Ukraine is an opportunity to reassess the risk levels and reflect on how this risk is covered in the audit plan:

Has the cybersecurity risk level been (re)assessed?

A quick scan could be useful to obtain an initial or an updated assessment on how well the organization is prepared against cyberthreats. A focus could be put on data breaches, continuity, and cybersecurity incidents which occurred over the last year.

Is the audit plan adequately covering the risk?

Ensure that the audit plan is still adapted and properly prioritized to take account of the dramatic evolving cyber risk exposure and existing threats on organizational and business developments.

Performing audits on cybersecurity

Internal Audit departments are often confronted with the need to evaluate areas where a certain level of technicality is required. It is essential to ensure the auditors' skill levels are adequate to provide a relevant assessment of the audited areas.

The fast pace at which the cyber threats evolve, the technical aspects of this risk and the size of internal audit teams can make it difficult or sometimes irrelevant for audit departments to maintain cybersecurity competencies internally. In this case, outsourcing may be an option, and many internal audit departments also rely on the second liners (especially the information security teams) for support.

In any case, CAEs must keep in mind that a good level of understanding on the nature of cybersecurity threats for their company is key to:

- Understand the risks and their possible consequences;
- Challenge the second line of defense (CISO), including on technical aspects, potentially with the support of external expertise;
- Raise relevant advice and recommendations to their stakeholders.

Conclusion

The Ukrainian conflict prompts a refresh of the cybersecurity practices. Organizations need to review and reinforce their security practices and improve their response capabilities. Cybersecurity should be managed as a risk discipline across the three different lines within the organization. Up to date risk indicators and report should be conveyed to the governance bodies so that they can direct, guide, and monitor the management. Audit and control functions can strongly contribute to achieve these goals.

References and Readings

Introduction & Context

Impact of the conflict in Ukraine on the level of cyber threat in Belgium

PME et cybersécurité dans le cadre du conflit russo-ukrainien : 7 conseils pour faire face aux menaces

Tensions internationales : renforcement de la vigilance cyber

UK government assess Russian involvement in DDoS attacks...

Preventive awareness

IT Risk Resources

Protecting Your Organization From Ransomware

What are the detection capabilities needs?

The Evolution of Security Operations and Strategies for Building an Effective SOC.

Protect, Detect and Correct Methodology to Mitigate Incidents: Insider Threats

What are the required response capabilities?

Book Review: Responding to Targeted Cyberattacks

DDoS Attacks–A Cyberthreat and Possible Solutions

Ransomware Response, Safeguards and Countermeasures

Cybersecurity Incident Response Exercise Guidance

What is the role of Internal Audit?

Risk in Focus

ABOUT

ISACA BELGIUM

ISACA Belgium (www.isaca.be) is a chapter of ISACA. ISACA® is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its more than 150,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through its foundation One In Tech, ISACA supports IT education and career pathways for under resourced and underrepre-sented populations.

IIA BELGIUM

IIA Belgium is affiliated to the Global Institute of Internal Auditors, based in the USA. The IIA is the standard and guidance setting body for the internal audit profession globally and promotes guidance following rigorous due processes. IIA Belgium is a non-profit professional organization dedicated to the advancement and development of the internal audit profession in Belgium.

IFACI

L'Institut Français de l'Audit et du Contrôle Internes (IFACI) gathers more than 6 500 audit, control and risk professionals. IFACI is affiliated to The IIA, global network of more than 220 000 professionals.

DISCLAIMER: ISACA Belgium, IIA Belgium and IFACI have designed and created this paper "The conflict in Ukraine: What do you need to know about cybersecurity?" primarily as an educational resource for IT security professionals, Internal Auditors and Controllers. All three organizations make no claim that use of any of this paper will assure a successful outcome. This paper should not be considered inclusive of all proper information, procedures, and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, IT security professionals should apply their own professional judgments to the specific circumstances presented by the systems or IT environment.

Authors

Philip De Picker

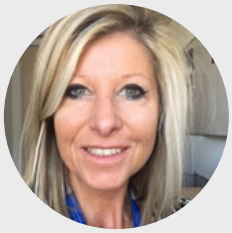
Secretary
ISACA Belgium

Egide Nzabonimana

Information Security Risk Expert
President ISACA Belgium

Valérie Schipman

GM, IT & Digital Internal Audit at Renault Group
IFACI



Katleen Seeuws

CEO
IIA Belgium

Patrick Soenen

DPO, Trainer
IIA Belgium

Olivier Sznitkies

Internal Audit and Information Risk Advisor at Audiligence
IFACI