The Need for Periodic Cyber Threat Simulation Exercises for University Staff

Avtandili Bichnigauri
Associate Professor, Georgian Technical University
bichnigauri_av@gtu.ge
Daviti Bichnigauri
Associate Professor, Georgian Technical University
davit.bichnigauri@gmail.com
Luka Shonia
Assistant Professor, Georgian Technical University
shonia@gtu.ge
https://doi.org/10.61950/giu.4.2026.12142

Abstract

Ensuring cyber and information security is one of the most critical challenges for modern universities. Universities, as open academic environments and centers rich in information resources, are particularly vulnerable to cyberattacks. This article argues that periodic implementation of cyber threat simulation exercises for university personnel is not a recommendation, but a necessary component for creating and maintaining organizational cyber defense. The article discusses the main types of simulations (phishing, ransomware, DDoS, incident response mechanisms), their technical support methodology and expected results. It is emphasized that periodicity allows not only to update knowledge, but also to implement a Continuous Improvement Cycle, which ultimately reduces risks and strengthens the overall security situation of the university.

Modern higher education institutions are complex organisms that combine educational, scientific and administrative functions. Their digital ecosystem includes personal databases of students and staff, copyrighted scientific research, financial documentation, learning process management systems and critical infrastructure. All this makes them an attractive target for cybercriminals. The openness characteristic of universities, decentralized IT infrastructure and constant turnover of staff and students create unique challenges for cybersecurity. Statistics indicate that more than 80% of crimes use social engineering methods, which is directly related to the low level of awareness of staff and users.

One of the most effective methods of solving this problem is the periodic implementation of cyber threat simulation exercises. Such exercises not only teach staff how to identify threats, but also create ongoing practical experience, which, unlike theoretical knowledge, is more firmly fixed. Periodic implementation of cyber threat simulation exercises is a strategic investment in the development of this capital. That is why every university should include simulation exercises as an integral part of its annual activity plan and allocate the necessary resources for this. This is a worthy investment in protecting academic freedom, research security, and the reputation of the entire academic community.

Keywords: Cybersecurity, Simulation Exercises, Phishing, Ransomware, Incident Response, Social Engineering, Awareness Raising, Continuous Improvement Cycle.

Introduction

Modern higher education institutions are complex organisms that combine educational, scientific and administrative functions. Their digital ecosystem includes personal databases of students and staff, copyrighted scientific research, financial documentation, learning process management systems and critical infrastructure. All this makes them an attractive target for cybercriminals.

The openness characteristic of universities, decentralized IT infrastructure and constant turnover of staff and students create unique challenges for cybersecurity. Often, even the most advanced technical protection systems cannot neutralize the human factor, which is the greatest weakness. Statistics indicate that more than 80% of crimes use social engineering methods, which is directly related to the low level of awareness of staff and users.

One of the most effective ways to address this problem is to periodically conduct cyber threat simulation exercises. Such exercises not only teach personnel how to identify threats, but also create ongoing practical experience that is more firmly established than theoretical knowledge. It is not only the fact that exercises are conducted that is important, but also their systematicity and periodicity, which leads to a process of continuous improvement and adaptation to new threats.

Methodology (main part)

A structured approach is necessary for the effective implementation of cyber threat simulation exercises. The proposed methodology includes the following stages:

1. **Risk assessment and definition of goals:**
   First of all, it is necessary to conduct a full audit of the university's IT infrastructure and data systems. The most critical assets (e.g., scientific research archives, financial records, personal data) and the threats to them are determined. Goals can be: increasing resistance to phishing by 25% in 6 months, testing the Incident Response Plan (IRP), familiarizing staff with the threat of ransomware, etc.
2. **Identification of target audiences:**
   It is worth noting that not all employees are at the same risk. It is necessary to define the appropriate target groups:
   - **Administrative staff:** works with financial and personal data. For them, simulation of BEC (Business Email Compromise) attacks is critical.
   - **Human Resources:** A frequent target for obtaining personal data of applicants.
   - **Faculty and academic staff:** Possess important intellectual property and copyrighted works. Simulations of scientific espionage and doxing are relevant for them.
   - **IT department employees:** For them, exercises should be technical - prevention of DDoS attacks, analysis of malicious software, activation of IRP.
3. **Selection of the type of simulation:**

- **Simulation of phishing campaigns:** Specialized platforms are used (e.g., KnowBe4, Proofpoint Security Awareness). Realistic e-mail templates will be created that imitate messages from the university administration, a bank or a popular service. Hyperlinks will be directed to a controlled website. Participants' actions (email opening, link clicking, data entry) will be recorded in the system.
- **Ransomware attack simulation:** harmless files are used that mimic ransomware behavior (e.g., simulating file encryption and displaying recovery instructions). This helps staff recognize signs of an attack and know what to do (disconnect the computer from the network, contact IT, etc.).
- **Tabletop Exercises:** These are situational games in which participants (usually management and IT specialists) jointly discuss and resolve a cyber incident created according to a scenario. For example, "Your university has discovered an encrypted file in the system with a ransom note. How will you act? Who should be involved? How will you inform students and the public?"
- **DDoS attack simulation:** Conducted under controlled conditions by the IT department, on test servers, to test the network's resilience and the effectiveness of mitigation mechanisms.

4. **Implementation and monitoring:**
   Exercises are conducted either announced in advance or suddenly (which is more realistic). The actions of all participants are monitored and recorded for analysis.
5. **Analysis and feedback:**
   After the exercise, data analysis is conducted: click rate, percentage of data entry, response time. Individual analytics are set for each participant and appropriate recommendations are prepared on what they clicked on, why it was a threat, and how to recognize a similar incident in the future. Those employees who "interfered" in the simulation process are required to undergo additional training.

Discussion

The periodicity of cyber threat simulation exercises is a critical factor that determines their long-term effect. One-time training, even very intensive, does not produce sustainable results. The reasons for this are as follows:

1. **Human psychology and retention of awareness:** People gradually forget what they do not use, and therefore, cyber threat knowledge is no exception. Periodic simulations constantly remind personnel of the existence of threats and create a defensive mentality against new threats. This is a process of constant renewal that prevents knowledge from becoming obsolete.
2. **Evolution of cyber targets:** Cybercriminals are constantly updating their tactics, techniques, and procedures (TTPs). Phishing techniques that were effective a year ago may be outdated today. Periodic simulations allow the university to flexibly respond to these changes and conduct new types of attacks in training scenarios, such as mobile malware, QR code phishing (Quishing), sophisticated phishing created by generative artificial intelligence, etc.

3. **Continuous Improvement Cycle:** Simulations are not only a training tool, but also a diagnostic tool. The results of each exercise provide unique data on the organization's vulnerabilities.
   - **First exercise (Q1):** reveals that 40% of staff clicked on the phishing link.
   - **Training and intervention:** Special training and individual consultations are conducted.
   - **Second exercise (Q3):** The rate drops to 15%.
   - **Analysis:** 15% is still high. The analysis shows that this group is mainly represented by non-technical employees. More targeted and easy-to-use training materials will be developed for them.

   In this way, the periodicity of exercises allows the organization not only to measure progress, but also to refine its cybersecurity strategy and resource allocation.

4. **Establish a culture of incident response:** When a real cyber incident occurs, panic and chaos often cause more damage than the attack itself. Periodic exercises and simulations create the so-called "muscle memory". Staff automatically start thinking: "This email is suspicious, I better check with the organization's CISO (Chief Information Security Officer)" or "The system is down, it could be a DDoS attack, I will act according to the IRP". This culture of proactive and coordinated response is more valuable than any single technology.
5. **Risk reduction:** The main goal of simulations is to turn a person into the strongest link in the security chain, taking him out of the weakest. Periodic training reduces the likelihood of simple mistakes (sharing passwords, leaking sensitive information) and reduces the overall number of successful attacks.

Results

After conducting cyber threat simulation exercises on a regular basis, the university can expect the following real and measurable results:

- **Increased phishing resistance:**
  Reduced click-through rate (CTR) from 40% to less than 10% after an intensive six-month program.
- **Reduced incident detection time:**
  When staff proactively notify IT of suspicious activity, incident detection and isolation are significantly accelerated. For example, during a real ransomware attack, the first notification to IT is received within hours, not days.
- **Increased effectiveness of the Incident Response Plan (IRP):**
  As a result of the exercises, the IRP becomes more sophisticated and practical. Communication gaps are identified, areas of responsibility are defined, and actions are more coordinated.
- **Optimize cybersecurity spending:**
  Exercises show where the greatest need for investment lies. Finances can be redirected to protect the most vulnerable segments, instead of scattering resources across all potential areas.
- **Change in organizational culture:**

Cybersecurity becomes everyone's business, not just the responsibility of the IT department. An environment is created where employees are not afraid to admit when they make a mistake and ask for help.

Conclusion

A university, as a center of knowledge and innovation, cannot remain unprepared for cyber threats. Technological solutions such as firewalls, antivirus and Intrusion Detection Systems are necessary but not sufficient. Human capital remains the last barrier and, at the same time, the first line of defense.

Periodic implementation of cyber threat simulation exercises represents a strategic investment in the development of this capital. They combine education, practice and continuous monitoring in a single flexible and adaptive framework. Such a program not only reduces the likelihood of specific cyber risks, but also creates a more resilient and cyber-aware organization.

Periodicity is key. It ensures that knowledge does not become obsolete, skills are not lost and the organization is constantly prepared for new and more sophisticated threats. Therefore, all universities should make simulation exercises an integral part of their annual activity plan and allocate the necessary resources for it. This is a worthy investment in protecting academic freedom, research safety, and the reputation of the entire academic community.

References

1. Bichnigauri, I. Kartvelishvili, L. Shonia - "Development and Implementation of an Effective Mechanism Model for Preventing Phishing and Malicious Code Websites in a Web Browser Environment", Georgian Technical University International Scientific-Practical Conference "Modern Challenges and Achievements in Information Technologies - 2023"
2. Bichnigauri, I. Kartvelishvili, L. Shonia - Unveiling Quishing: The Dark Side of QR Codes in Cyber Attacks, Journal "Defense and Science". Vol. No. 2 (2023), DOI: https://doi.org/10.61446/ds.2.2023.7412
3. Bichnigauri, I. Kartvelishvili, L. Shonia - Strengthening Cyber Defenses - The Crucial Role of Phishing Simulation in Modern Security Strategies, Journal "Defense and Science". Vol. No. 3 (2024), DOI: https://doi.org/10.61446/ds.3.2024.8467
4. Bichnigauri, O. Shonia - "Means for Detecting IoT Devices in a Local Network to Ensure Their Cybersecurity", Scientific Papers. Automated Control Systems. № 1(32), Vol.1. Tbilisi, 2021
5. Bichnigauri, O. Shonia, T. Kaishauri - "Detecting Suspicious Domain Names for Cyber Threat Identification Using CTL Technology", International Scientific-Practical Conference "Innovations and Modern Challenges - 2022" dedicated to the 100th anniversary of the Georgian Technical University and the 65th anniversary of the Faculty of Information and Communication Technologies, Tbilisi, 2022
6. Strategy for Raising Awareness in the Field of Cybersecurity for 2025-2030 - https://dga.gov.ge/files/mUMPR8s3w59z.pdf
7. ENISA (European Union Agency for Cybersecurity). (2021). Cybersecurity Education in the EU.

8. Law of Georgia on Information Security - https://matsne.gov.ge/document/view/1679424?publication=8
9. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
10. NIST Special Publication 800-50. Building an Information Technology Security Awareness and Training Program.
11. SANS Institute. (2023). The Human Element in Cybersecurity: Annual Report.
12. CISA (Cybersecurity and Infrastructure Security Agency). (2023). Security Awareness Training Best Practices.
13. ENISA (European Union Agency for Cybersecurity). (2023). Cybersecurity Culture Guidelines for Organizations.
14. Kovacevic, A., & Veinovic, M. (2022). The Role of Tabletop Exercises in Improving Organizational Cyber Resilience. Journal of Information Security.
15. Hadlington, L. (2018). The Human Factor in Cybersecurity: Exploring the Accidental Insider. Psychology Press.