Cyber Security at MONETA Money Bank, a.s.

As part of its business strategy, MONETA Money Bank, a.s. (“MONETA”) is accelerating its transformation of services to become the digital leader in distribution of financial products. Naturally, new progressive technology is involved to help achieve the goal. However, technology alone cannot address the vast amount of cyber threats that confront organizations. Maintaining security in the digital world requires more than just the right technology. Therefore, MONETA incorporates a holistic approach of technical, human and physical factors to detect, prevent, and correct cybersecurity-related issues.

Cyber Security Strategy

MONETA has established a mid-term cyber security strategy, which is endorsed and followed by the Management Board of MONETA and is reviewed yearly to adjust to the relevant objectives of the business strategy. The cyber security strategy of MONETA is strongly based on the foundation of the following three pillars:

- Governance,
- Risk management,
- Compliance management.

Cybersecurity governance is a critical element of awareness and the defensive building block upon which all other security measures rest. Concise rules and accountability define clear policies and procedures. In order to broaden cybersecurity competencies, information security risks are continuously managed by repeatedly:

- Specifying security objectives,
- Assessing risks and controls,
- Implementing treatment plan,
- Monitoring and reviewing the performance,
- Maintaining and improving the process.

As an organizational unit of MONETA, the cybersecurity team achieves the defined strategy goals by:

- Communicating accurate risk landscape to the top management,
- Periodically performing risk assessments,
- Issuing security policies, guidelines and procedures,
- Providing guidance and assurance in implementing controls and measures,
- Monitoring adherence to controls using suitable tools,
- Investigating emerging threats and security trends,
- Acting as a second line of defence (IT being the first),
- Effectively managing cyber security incidents,
- Increasing cyber security awareness within the organization.
Monitoring and Incident Management

To ensure reliability, availability and security of business services within an increasingly complex IT environment, internal network traffic is constantly being monitored for anomalies using an advanced flow-based network traffic monitoring approach. Real-time analysis of generated security alerts and collected logs is provided by a Security Information and Event Management (SIEM) system, which is monitored by the 24x7 Security Operations Center (SOC). Alerts and incidents are escalated to Incident managers, who follow the incident end-to-end and make sure that not only the incident gets resolved, but lessons learned are also identified and implemented.

Vulnerability Management and Penetration Testing

Regular assessments of cyber security became an organic part of internal security program a long time ago. To remain up-to-date, the scope and methodology is constantly updated as new threats and vulnerabilities emerge. Concise, actionable findings and effective remediation recommendations are enabled by appropriate security metrics and information gathered within regular tests, i.e.:

- Penetration testing to enable full risk assessments of network systems by both an internal team as well as external security auditors to assure results objectivity;
- Vulnerability scanning to automate known-vulnerabilities and system misconfiguration tests including missing patches, default/common password verification and Denial-of-Service (DoS) resiliency tests.

Regulatory Compliance and Auditing

Focused on business goals and core competencies, MONETA incorporates policies and procedures, encompassing risk assessment and management, regulatory and audit compliance, as well as business continuity planning while keeping up with regulations, the latest requirements, and best practices from a cybersecurity standpoint.

Furthermore, MONETA cooperates with national regulatory authorities and follows international standards to fully comply with national and international policies and requirements, namely Czech National Bank legislation, Payment Cards Industry Data Security Standards (PCI DSS), EU GDPR, etc. In order to remain independent, both internal and external auditors are involved to provide an even more objective view of cyber security. Information Security policies and systems are audited on a regular basis. In 2017, there were several instances of audits examining the information security processes of the bank:

- Annual audit by an independent auditor, where IT Security is included in scope;
- In-depth audit by the Czech National Bank;
- Internal audit performs regular audits verifying IT Security processes;
- 360° Security Assessment conducted by an independent vendor.
Vendor Management

MONETA diligently selects external resources via a highly documented process to monitor and perform assessments on vendors and external outsource providers which manage, process or store confidential information. In order to minimize the risk and to evaluate their security status, the process naturally incorporates multiple departments (Legal, Compliance, etc.) to define the correct contractual requirements and agreements.

MONETA seeks to leverage the benefits of cloud services that are highly secure and compliant data centres and network architectures which are able to provide scalable innovative digital platforms within a secure environment and that meet the requirements of the most security-sensitive organizations. With cloud services, we cooperate with the regulator (the Czech National Bank) very closely to make sure we do not step outside of regulatory boundaries.

Training & Awareness

Due to a lack of realization that cybersecurity is a multi-disciplinary responsibility shared throughout the organization, many organizations learned the hard way that humans represent the weakest link in cybersecurity defences. Therefore, thorough training programs have been developed in order to raise awareness and help employees as well as clients navigate, survive and thrive in the digital wilderness, make informed decisions, and to successfully recognize and deal with various types of possible threats. MONETA promotes a positive security culture by analysing its leadership, HR policies and practices, IT governance, physical defences, and the cybersecurity awareness and accountability of its staff, its partners and contractors. A strong organizational culture and morale, supported by a strong cybersecurity education program, combined with teamwork, collaboration, and loyalty create an incredibly powerful security measure.
Examples of mandatory trainings on cyber security, data protection and privacy are as follows:

<table>
<thead>
<tr>
<th>Training</th>
<th>Description</th>
<th>Frequency</th>
</tr>
</thead>
</table>
| **Induction**                                 | Full day classroom training, containing among others:  
- IT Security: data classification, security incidents, password management;  
- Data protection: personal data protection legislation, banking secrecy;  
- Inside information protection.                                                                                                                         | Upon joining the company |
| **IT Security**                               | Quarterly mandatory “refresher” on secure behaviours (e.g. e-mail security/phishing threat).                                                                                                                 | Quarterly (e-learning) |
| **Personal Data Protection, Banking Secrecy and Trade Secrets** | - Intro to legislation governing personal data;  
- Responsibilities and liabilities of the bank and of the employee;  
- Processes employees must observe to prevent non-compliance.                                                                                      | Annually (e-learning) |

Furthermore, IT Security and Compliance awareness initiatives are reinforced by regular communication campaigns on specific topics (e.g. mobile device security, data protection, etc.), see samples below:
Privacy and Data Security

In banking, trust and confidentiality are essential. At MONETA we strive to achieve the maximum protection of the data in our custody, especially client data.

As MONETA is a publicly traded company, we also set up rules for management and protection of inside information in our internal policy. All employees are obliged to pass the training on the annual basis (first training must be passed after joining the company).

Data Protection

MONETA enforces data classification for the data in its custody. Mandatory encryption at-rest and in-transit are applicable to any data classified as Confidential or higher. Special attention is dedicated to personal data and sensitive personal data. As MONETA operates in the EU, it is fully subject to the General Data Protection Regulation, and therefore meets its strict requirements for handling and managing personal data.

Data Loss/Leakage Protection

Data stored on endpoints, especially from lost or stolen equipment, has always been an interesting target for attacker attempts to gain access to valuable data. In order to meet compliance requirements and to prevent the theft of personally identifiable information (PII) or sensitive personal information (SPI), MONETA leverages a powerful software component composed of several protection suites, which provides:

- Strong access control and data encryption,
- Certified encryption technology,
- Support for mixed-device environments.

In conjunction and to further enforce policies for compliance, privacy, and intellectual property (IP) protection, a market-leading data loss prevention (DLP) solution has been deployed company-wide. USB data and removable device access are protected and controlled using a state-of-the-art DLP solution, which protects against unauthorized usage of valuable company data by hardware and content-based filtering, monitoring and blocking of confidential data on any removable storage device.

Compliance Monitoring

Having internal policies and requirements to comply with external regulatory mandates would be ineffective without enforcing them. MONETA incorporates technological solutions to automate the
assessment of security and compliance controls in order to demonstrate a repeatable and trackable process to auditors and stakeholders. Assessing procedural and technical controls for vendor risk management, internal IT compliance and general best practices is assured by:

- Configuration management to perform security configuration assessments on systems throughout the network;
- Patch management to update, fix, or improve operating systems and other software, and improving their usability or performance as part of lifecycle management.

**Business Continuity**

The security incident management process in conjunction with business continuity plan (BCP) are fully capable of addressing adverse scenarios related to cyber security (a data breach, DDoS, a ransomware attack, etc.)

MONETA implements advanced policies to further protect its assets:

- Disaster recovery is in place to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster via integrating a BCP;
- Cyber insurance policy to limit exposure from Internet-based risks, and more generally from risks relating to IT infrastructure and activities;
- Vendor management to find strategic partners that can help achieve the desired business goals and resilience.