G7 FUNDAMENTAL ELEMENTS OF RANSOMWARE RESILIENCE FOR THE FINANCIAL SECTOR

October 2022

The growth and proliferation of ransomware is one of the most significant challenges that financial entities currently face. Ransomware manipulates a compromised information system for the purpose of extortion, such that the victim cannot entirely use the system or the data stored on it until a ransom demand is satisfied.[1] Ransomware by its nature impacts the ability of victims to continue their business operations. For the financial sector, ransomware can pose an unacceptable risk.

Ransomware attacks may not stop until their use is no longer profitable. It is important that financial entities take the necessary steps to make themselves resilient to ransomware before an attack occurs. In doing so, they should also consider risks to critical third party providers, which have the potential to create direct or indirect ransomware risks for financial entities. Addressing these issues will help financial entities preserve business operations and avoid making ransom payments that could motivate attackers to continue to seek profits from ransomware attacks.

This document provides financial entities with high-level building blocks for addressing the ransomware threat. It is non-prescriptive and non-binding, and is meant to incorporate the current policy approaches, industry guidance, and best practices in place throughout the G7 member countries. While focusing primarily on private sector financial entities and their critical third party providers, this document may also be used by financial authorities for their own internal ransomware mitigation activities as well as their efforts to promote the resilience of the financial sector.

The steps to create resilience against ransomware, in many cases, should resemble what entities have already been implementing to prepare for cyber incidents. The *G7 Fundamental Elements of Ransomware Resilience for the Financial Sector* document aligns with the *G7 Fundamental Elements of Cybersecurity* document that was released in 2016. For each element presented in the original document, this document describes the considerations that are essential to addressing the ransomware threat.

Element 1: Cybersecurity Strategy and Framework
Incorporate ransomware resilience within the entity's overall cybersecurity strategy and framework.

An overarching cybersecurity strategy and framework are necessary components of any cybersecurity program in any organization. Together with other threats being considered by a financial entity, the risk of ransomware is best treated with an integrated and comprehensive approach.

[1] For the purpose of the document, the definitions of key terms refer to the Financial Stability Board (FSB) Cyber Lexicon unless otherwise specified. An update of the FSB Cyber Lexicon (2018) is in progress and a revised version is expected to be published in 2023. The revised version is expected to include an agreed definition of ransomware, which did not have its own standalone definition in the 2018 Lexicon.

Most successful ransomware attacks involve a breach allowed by inadequate cyber hygiene practices within an organization. This may include lack of strong authentication practices, inadequate end user cybersecurity and anti-phishing training, inadequate asset management, lack of effective network segmentation, or slow or incomplete vulnerability patching on critical assets. These vulnerabilities are usually addressed within the financial entity's overall cybersecurity strategy and framework.

Element 2: Governance

Ensure effective coordination for the broad organizational impacts of ransomware through effective governance structures.

Ransomware incidents are rarely confined to the information technology functions of an organization, but rather carry with them significant implications for business operations, legal and regulatory compliance, marketing, and public affairs functions. It is important to develop a strong enterprise cybersecurity governance that incorporates ransomware planning within the overall decision-making processes. Such preparation includes Board of Directors-level oversight and a high level of coordination across business units. Governance discussions may address such issues as asset tracking, data classification and backup strategies, exercises, vulnerability scanning, and end-user cybersecurity training, all of which are important to protecting against ransomware as well as other cyber threats. Further important topics of senior-level governance discussions related to ransomware are:

Planning for Ransom Demands – G7 countries generally discourage ransom payments, which may help finance criminal enterprises and provide unintentional incentives for continued malicious behavior. Ransom payments do not guarantee restored data access, given the possibility that the private key cannot be obtained or that data restoration using that key is unacceptably slow or incomplete. Attackers may also retain copies of sensitive data captured in a ransomware attack that may give them continued leverage over a victim.

Ransom payments may be discouraged by national policy or industry standard. In some cases, ransom payments may be legally prohibited, such as when they involve payments to an entity designated for economic sanctions. Entities should consider reviewing the laws of their particular jurisdiction prior to a ransomware incident. Entities should also consider that there might be difficulties in identifying the attacker or recipient of a ransomware payment to assess potential sanctions risks.

Business Continuity Planning – Ransomware incidents can disrupt critical information systems for extended periods of time, potentially causing significant impacts to critical business operations. Cybersecurity professionals within the organization will benefit from collaborating closely with other operational components on business continuity planning considerations. They should consider including ransomware scenarios within their business continuity plans.

Communications Planning – Internal and external communications plans are additional items that are best addressed through senior-level deliberation. Financial entities rely heavily on trust as a core part of their business. Financial entities will want to anticipate the interests and concerns of key

stakeholder groups so they can be addressed through timely and effective communication. This may include customers, business partners, employees, supervisors, and the general public.

These groups may have concerns over the impact of the ransomware incident on the ability of the affected financial entity to continue to provide services as well as on the security of account holdings and personal and firm data. They may also have questions regarding the entity's response to payment demands.

Cross-Organizational Planning – In addition to high impacts on an individual entity, ransomware incidents within the financial sector may have the potential to create significant impacts that cut across a broad range of other financial sector entities and their customers. Financial entities, industry organizations, and financial authorities play important roles in establishing sound structures through which ransomware risk can be addressed. Effective cross-organizational planning will clearly identify roles, responsibilities, and coordination mechanisms for various levels of decision-making. These may include a diverse group of stakeholders, including regulatory authorities, law enforcement and cybersecurity agencies, insurance providers, emergency response teams, and even novel stakeholders such as virtual asset service providers.

Element 3: Risk and Control Assessment
Ensure the application of controls to address ransomware risk.

Financial entities benefit from assessing their ransomware risks and compensating controls within their existing cybersecurity framework and from identifying third party providers (including cloud services such as storage and e-mail) that may be entry points for cyber threats. Financial entities benefit from awareness of third party cybersecurity practices and any incidents they may experience.

Entities may seek to address ransomware risk in part through the purchase of insurance policies. Insurance policies can protect businesses from some ransomware-related losses, in particular recovery losses. Many policies also provide access to a broad range of response resources, including breach coaching, attacker communications, public relations, and forensics. Insurance policies are not a substitute for strong cyber hygiene and effective counter-ransomware planning, and in fact many insurers require evidence of these as part of their underwriting process. Policies come with limitations, deductibles and sub-limits, and exclusions, and will typically not cover full financial losses. For example, severe negative outcomes of ransomware such as reputational and compliance impacts are extremely difficult to insure against.

Element 4: Monitoring
Monitor systems for signs of potential ransomware activity.

Indicators of ransomware activity are best identified through the intrusion detection systems and related systems that a financial entity has in place for detecting malicious or anomalous activity on their information systems. There are a variety of sources of information that organizations can use to track external ransomware threats and seek to identify trends. These information sources include threat reports and intelligence feeds issued by law enforcement and cybersecurity agencies, industry bodies, and third party security providers, among others.

Element 5: Response
Implement established plans in response to ransomware incidents.

Entities will be most effective in their ransomware response when they operate on multiple levels in a coordinated fashion. It is important that entities make a continuous effort to enhance their systematic responses through trainings using multiple scenarios that reflect different aspects of ransomware impacts.

Ransomware incidents can amount to crimes and may require coordination with appropriate competent authorities. Financial entities benefit from establishing relationships with appropriate law enforcement, national security, and regulatory authorities prior to a ransomware incident to facilitate communication during an incident. Depending on jurisdiction, a financial entity may be able or required to report suspicious activity that may be indicative of a ransomware incident to competent authorities.

Many organizations will rely on third parties to assist them in their ransomware response activities. The use of third parties allows organizations to quickly augment their response capability through the support of trained personnel who are experienced in ransomware response. Financial entities should be advised, however, that for widespread incidents there may be a high demand for these services from multiple organizations at the same time. Entities may therefore consider identification of potential alternative providers as part of their response plan.

Financial entities may be asked to play a role in response to incidents that do not impact their particular systems. Ransomware payments are often made through financial entities, including through virtual currency exchanges. Financial entities play an important role in protecting the financial system from ransomware threats through compliance with their Anti-Money Laundering and Combating the Financing of Terrorism obligations, which include reporting suspicious activity related to ransomware. In addition, countries should implement the Financial Action Task Force Standards, in particular related to virtual assets, to reduce criminals' access to and exploitation of financial services.

Element 6: Recovery
Take steps to restore capabilities that may have been impaired by a ransomware incident.

An essential element of recovery from a ransomware incident will be backup and restoration of systems and data. In developing a data backup strategy, entities should consider the capabilities of ransomware actors to circumvent or disrupt common backup practices. They should consider that ransomware actors may seek to infect backup data and may start doing so long before the ransomware attack itself becomes apparent. This can make it difficult to restore data without re-infecting the entity's systems. Also, even if data are properly backed up and restored, attackers may hold exfiltrated data for extortion under the threat that the data may be publicly exposed.

Financial entities should consider backup strategies that possess characteristics that make them resilient against ransomware. These solutions may include systems that prevent the modification,

deletion, or encryption of stored data.[2] They may also include practices such as more frequent backups, longer periods of back-up retention, offline backups, and redundancy of data storage solutions across a variety of on-premises and off-premises systems.

As with their response activities, entities that have tested beforehand their backups and exercised and validated restoration of their data and reinstallation of critical user accounts and software within appropriate time objectives will be best able to recover from ransomware attacks. Data restoration is notoriously challenging, especially for large sets of data, and entities are likely to run into unexpected issues when they restore from their backups.

It is important for an entity to carefully document its recovery process, as such documentation may be needed by law enforcement investigators. It is also important to identify and document lessons learned that the entity may apply to future incidents.

Element 7: Information Sharing
Exchange data, information, and/or knowledge about ransomware incidents and trends with internal and external partners.

Ransomware activity often follows patterns based on malicious actors, targeted industry, tactics employed, and other factors. Entities should seek to understand these patterns in order to enhance situational awareness and continuously monitor for common vulnerabilities for remediation and new indicators of compromise.

Depending on jurisdiction, there may be mandatory reporting regimes for ransomware attacks. Entities should also consider making reports to competent groups such as intelligence and information sharing networks (e.g., Financial Cyber Security Incident Response Teams and Information Sharing and Analysis Centers).

Element 8: Continuous Learning
Increase ransomware resilience by learning from past incidents.

As for all cybersecurity issues, dealing effectively with ransomware requires adoption of a continuous learning approach. Since ransomware attacks are often associated with a lack of general cyber hygiene against sophisticated attacks, entities should consider devoting additional resources to on the training of end users, who can be susceptible to phishing, social engineering and other attacks that lead to unauthorized access of an entity's systems and generate weaknesses that ransomware can exploit. Additionally, ransomware threats are constantly evolving, as are the technologies to mitigate against them. Financial entities can maintain their ransomware resilience by tracking these changes in the threat environment, frequently reviewing system logs to ensure compliance with sound practices, and improving processes and configurations when failures are identified.

[2] Back-up technologies with some or all of these qualities are sometimes referred to as "immutable."