Response tactics in an evolving cyberthreat landscape

With a growing amount of international business being done online and in a virtual setting, world economies are becoming more reliant on safe, secure cyber environments. But these environments are under threat. Chris Dimitriadis of INTRALOT examines the dangers inherent in any cyber environment and discusses the need for up-to-date, robust controls and plans to help combat cyberthreats effectively.

By Chris K. Dimitriadis, Ph.D., CISA, CISM, CRISC
Group Director of Information Security, INTRALOT

Information Technology is the backbone of the world economy and an enabler of business innovation. The World Economic Forum has called the rapid proliferation of technologies "The Fourth Industrial Revolution[1], while a joint analysis of Accenture and Oxford Economics[2] revealed that digital technologies could add more than USD 1.3 trillion to the GDP of the world's top 10 economies by 2020. In the EU, the Digital Single Market Strategy of the European Commission[3] reports that the digitization of products and services could add EUR 110 billion to annual revenue in Europe within the next five years. Following these trends, the gaming industry is undergoing a digital transformation era to unlock its potential, blurring the line between the digital and physical worlds.

However, while this digital revolution is undoubtedly a significant leap forward, the introduction of new technologies and our increased dependence on digital goes hand-in-hand with an evolution in cyberthreats.

The global impact from cyberthreats is currently around USD 3 trillion per year and the average cost of a single attack is estimated at USD 4 million. Denial-of-service attacks cost anywhere from USD 50K to hundreds of thousands of dollars per hour and their sophistication increases rapidly, as recently witnessed through attacks launched by botnets consisting of Internet of Things devices[4]. The US Commission on Enhancing National Cybersecurity's 2016 report[5] underlines the risks inherent in the supply chain and those of increased complexity; this is of particular concern in markets that use multiple vendors to provide their services. Most of all, we have the rise of the Dark Web. This virtual hideout for cybercriminals uses anonymity networks to hide sites where one can rent botnets for denial-of-service attacks, procure ransomware as a service, and gain access to numerous tools for deploying different types of attacks.

Of necessity, regulation at the same time becomes stricter. This includes the new General Data Privacy Regulation in the EU, the Network and Information Security (NIS) Directive in Europe, the Cybersecurity Information Sharing Act in the US, and several regulatory reforms that increase liabilities in case of a breach. According to a recent study by ISACA Cybersecurity Nexus (CSX) and RSA[6], 80% of boards of directors are concerned about cyberthreats. This comes as a result of cyber breaches gaining increased visibility in the media, together with their direct financial impact, the drop in stock prices in the event of an incident, and the related increased direct board member liabilities.

But what is Cybersecurity all about? How do we respond when even major corporations and agencies in the most advanced countries have faced incidents?

Cybersecurity can be effective when holistically designed. When cybersecurity stops being simply about preventing attacks, and starts becoming about being able to detect, respond to and eventually recover the organization from an attack, only then can Cybersecurity serve business effectively. This is clearly depicted in the recently published US-NIST Cybersecurity Framework[7] that separates cybersecurity into five main services: Identify, Protect, Detect, Respond and Recover.

INTRALOT Cybersecurity Unit has implemented the key concepts of the US-NIST Framework as detailed here.

In brief, "Identify" relates to the organization's capability to understand and prioritize

1 https://www.weforum.org/focus/the-fourth-industrial-revolution | 2 https://www.accenture.com/us-en/insight-digital-density-index-guiding-digital-transformation | 3 https://ec.europa.eu/digital-single-market/en/digitising-european-industry | 4 https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/ | 5 https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf | 6 http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf | 7 https://www.nist.gov/cyberframework

its needs, based on effective risk management frameworks. It is about focusing on the important assets and the business environment. In the lottery industry, this relates to gaming transactions, ticket security, player behavior, player personal data, and internal user activities, among others, that differentiate the attack surface. This also relates to the whole supply chain for ensuring player and stakeholder trust and compliance.

"Protect" is about the technical, procedural, organizational, human and culture-related measures for preventing attacks, from network, operating system, database, and application controls, to training and awareness and third-party (i.e. Cloud or service provider) controls for protecting the lottery. Technical controls should be embedded in the solution of the technology provider, while the lottery operator should ensure trained employees and management commitment to cybersecurity.

"Detect" is about the systems and processes for identifying incidents, through processing of logged events and through real-time monitoring of data and transactions. This service requires both technical capacity to log and display events in a prioritized manner, and cybersecurity expertise and processes for detecting attacks in a timely manner.

"Response" and "Recovery" are the areas in which many of the participants in today's digital economy have put the least focus. They are, however, two crucial cybersecurity services and must be addressed and given high priority.

Response tactics differ, based on the nature of the incident, but whatever the case, the organization needs a team, a plan and pre-established contacts with external parties. The response team must be a group of cybersecurity experts with the capacity to analyze and mitigate the attack. The analysis should expose the affected systems and business impact, but, most importantly, the type and duration of the attack. For example, a breach could be new, but could also have been present for the past few months or years if detection failed to identify it in a timely manner. In the latter case, analysis could take much longer and the impact would most probably be orders of magnitude higher. Attack mitigation is about stopping the attack without removing traces for identification purposes, as well as avoiding propagation to other systems. The team actions should be guided by a written and tested response plan that describes the roles, systems, procedures per incident type; communications with stakeholders, authorities and the press; as well as contacts with third parties such as suppliers and external cybersecurity experts for aiding the team (e.g. forensics services). Incident reporting, testing, and improvement are also important elements in terms of the effectiveness of the response plan.

Chris K. Dimitriadis heads information security, information compliance and intellectual property protection at INTRALOT Group. He has built INTRALOT's Global Information Security operations and is now responsible for the alignment of the group's security strategy with business needs, and oversight of its execution.

"Recovery" planning can be part of the overall business continuity plan. It requires roles, procedures, communication, and technical controls in order to recover a system. For example, if the organization suffers a ransomware attack, backups are crucial for being able to restore data. In the case of denial-of-service, a series of technical controls and agreements with Internet Service Providers are crucial components. Most of all, testing the plan is a vital control towards ensuring readiness.

If cybersecurity seems complex or costly, there is always the option of outsourcing. What cannot be outsourced though, is a core team of senior cybersecurity experts for developing and implementing the lottery's cybersecurity framework, as well as for managing security suppliers and linking their services with the business.

What is absolutely critical with cybersecurity is that it is not disregarded – which is highly unlikely in a regulated market like the lottery one. What is even more important is that it is not only partially implemented. The latter could lead to even worse consequences, as a false perception of security leads to unregistered risk and subsequently in transforming trust into a game of luck.