Dealing with the Increase **in Cybersecurity Threats**

by Robin Williams, CISA, CDPSE, CIA IT Lead
Robin@grippadvisory.co.za

Introduction

Since the start of the covid-19 pandemic in 2020, security researchers have estimated that cybersecurity attacks have increased by 300%[1], with over 45 000 hack attempts occurring every day in South Africa[2]. The increase in number is driven primarily with the fast adoption of digital transformation to enable remote working from home, the establishment and increase of hacking forums where information about vulnerable organisations are exchanged, and due to the profile of the typical hacker evolving with the establishment and accessibility of automated penetration test tools allows any interested person to become a hacker.

Another alarming prediction is that the total cost for cybercrime committed globally will reach $6 trillion in 2021, up from $3 trillion in 2015[3].

Why is cybersecurity important for gambling operators?

Gambling operators, including online and land-based casino operations, Limited Payout Machine (LPMs) and Bingo operators have been a target for scammers and fraudsters since the early days of gambling. Criminals tend to follow the flow of money, and with significant money changing hands in the gambling business, it has always been a natural fit to target these operations. So much so, gambling operators have become synonymous with high-level security, employing secure networks over its operational gaming systems and employing teams of loss prevention / security officers in and around the gambling floor to limit the risk.

As gambling operators do an increasing amount of business online, the threat from scammers remains relevant, if not heightened from before – only the landscape has changed. So instead of chip switching scams, hidden earpieces and heists, we see denial of service (DoS) attacks, game hacks and fraud involving user accounts (i.e., stealing confidential and payment information).

Cybersecurity is an increasingly big issue for gambling operators, if not more important than security at land-based gambling operations. With a more condensed target, and various ways to potentially penetrate digitised systems, gambling operations need to be more proactive than ever to secure their platforms.

With the rise of hacking forums on the internet and information available on the dark web regarding the trade of compromised accounts and / or backdoors into gambling networks, gambling operators need to incorporate threat intelligence into their security plans to identify emerging, unknown threats and attacks that can be launched against their organisations and react promptly to this information before it turns into a breach.

Risks of Hacking

It's important for gambling operators to take measures to prevent loopholes and exploits from giving criminals or attackers access through the back door. If a gambling operation is vulnerable, it's potentially exposing the personal details of its customers to the fraudsters, who could then use this data to steal either directly or indirectly from the customer or the operator.

Privacy legislation such as POPI or the European variant called GDPR, requires organisations including gambling operators to design their systems and processes with privacy and security in mind. These regulators put all organisations to the test when it comes to cybersecurity posture and effectiveness and requires disclosure of any data breaches as soon as they become apparent, which is a public relations disaster waiting to happen. There may also be licensing issues for those found wanting.

And of course, it does nothing to build trust between the customer and their chosen gambling operator, if online operators are vulnerable to these types of attacks. This has potentially longer-term implications for gambling operators, and as we have seen with high profile hacks in years gone by, there's the very real potential of destroying a trusted gambling operator brand.

Unfortunately, this is not a static picture either, with the risks and defences in cybersecurity constantly changing and evolving. As a result, it's essential that gambling operators take the risks seriously and take steps to protect against these threats both now and in the future.

What control measures can you put in place to prevent cyber related security incidents?

During the Cold War, US President Ronald Reagan adopted a signature phrase – 'trust but verify' – in delicate negotiations with the Soviet Union. This was a great framework to ensure that both East and West complied with the conditions of the nuclear disarmament treaties.

Absolute security has always been an impossible goal, but there is a need to adopt a new framework to truly minimize business risk. The current digitally transformed world has created a completely dynamic environment where a static trusted state cannot be assumed. This requires a rethink of Reagan's mantra. Now a 'verify and keep verifying' approach is needed. This zero-trust attitude to network security means that one cannot make any assumptions, and one has to continually authorise and protect organisations and their people, their assets and their workloads.

Continued on page 30

[1] *Internet Crime Complaint Centre (IC3) as reported by wwwthehill.com*
[2] *Research from Kaspersky on South Africa cyber trends*
[3] *Kaspersky global report on cyber crime*

Dealing with the Increase **in Cybersecurity Threats**

Continued from page 28

An organisations effort needs to tackle cyber security holistically covering the people, process and technology elements of internal control, while having a good balance of preventative (controls to prevent cyber risk from occurring) and detective controls (mechanisms to identify breaches when they happen) to effectively manage cyber risk. The implementation of best practice Information Security Management Systems (ISMS) or security program is a good starting point in tackling cyber risk and applying the zero-trust principle, which is incorporated in nearly all ISMS frameworks. The benefit of adopting a best practice security framework is that the organisations that have designed these frameworks continuously research the threat landscapes and ensures that their frameworks are relevant to tackle the latest threats and vulnerabilities available.

The foundational and baseline practices organisations should consider and can implement to provide basic level of protection to cyber risks are:

Detection, Response and Mitigation
Security incidents can happen without warning and they often go undetected for long periods of time. On average, it takes organisations 6 months to detect a breach after an initial compromise[4]. Detective controls are important in the fight against cybercrime and it is important that security teams have systems and processes in place to review security logs generated to identify suspicious activity in a timely manner. The time taken to detect a breach has financial implications, with faster detection rates decreasing the costs.

A security incident response plan should be developed and accompany the detection efforts detailing the steps to contain and control a security related incident to prevent further unauthorised access to data and information.

Vulnerability Management and Penetration Testing
A vulnerability assessment is an automated technical assessment designed to find as many flaws as possible in a computer environment.

Organisations should enable continuous vulnerability scans to identify and remediate any vulnerabilities that can be exposed by an attacker. This should be supplemented with recurring penetration tests to monitor security exposures and evaluate the effectiveness of the security team's response to a security incident.

Patch Management
20% of breaches recorded occurred because systems were running outdated software that had known security vulnerabilities. It is important that organisations ensure that all systems remain up to date and are patched as soon as security patches become available.

Configuration Review
All devices connected to an organisations network should be configured according to a best practice baseline to sufficiently harden the network and stay up to date with the latest security trends.

Awareness and Security Training
Staff are normally considered the weakest link when it comes to cyber security as initial attacks are targeted towards employees through phishing campaigns.

Organisations should continuously train staff on security risks and conduct routine social engineering and security breach simulations to improve security behaviours.

End Point and Perimeter Protection
It is important to ensure that anti-virus protection is enabled to protect all endpoints and firewalls with intrusion detection (IDS) and protection services (IPS) to prevent malicious and harmful traffic coming into the organisations network. Firewall rules and configurations should be regularly reviewed to ensure that weaknesses in the security of the network will be found prior to exploitation and allow rules to be updated as necessary to meet technology changes or new threats.

Cyber Security Reviews
It is important to continuously review your information security practices for gaps or deficiencies to ensure that the network and connected devices are sufficiently hardened to protect against cyber-attacks, and that the organisation have adequate protection from cyber risk.

A combination of internal assessments performed by the security team together with expert companies specialising in cybersecurity assessments should be used to continuously assess the effectiveness of cybersecurity controls in place. A cyber security review is a comprehensive audit focusing on reviewing the adequacy and effectiveness of the people, process and technology arrangements in place dealing with cyber risk, and incorporates validating the controls through the performance of penetration testing and vulnerability analysis.

Conclusion

Managing cybersecurity or, more specifically, managing cybersecurity risk, is much more than just technology and, in most cases, has nothing to do with having the money to afford state-of-the-art technology.

Managing cybersecurity risk is generally a matter of acquiring affordable technology and, above all, getting the basics right: managing people, processes and organisation, and setting up governance and operational models (i.e. security framework) that work. This is easily said but is a big challenge by itself, particularly in larger organisations where several teams and service providers are involved, each of them with a specific service level agreement. The more pieces in the puzzle, the more complex it becomes, and the reality will prove that defining and improving security related roles, responsibilities and processes in organisations will turn out to be more valuable than implementing next-generation firewalls and technology acquired by the organisation to address cyber risk.

There is no magic solution, nor a single approach that fits all. Knowing the organisation, the industry in which it operates, the risk and the resources will result in a better position to develop the right solution.

[4] *Research from Kaspersky*