EBOOK

Countering Emerging Security Threats in Lottery

How You Can Mitigate Security Risks in the Modern World

BULLETPROOF

a GLI® company

Introduction

Technology continues to evolve as do cyber criminals. The lottery industry has transformed with innovation and faces ever-growing challenges and risks. With new platforms, integrations, vendors, and delivery adapting to serve a consumer-centric market, lotteries can offer novel ways to attract new players, extend their reach, and generate more for the worthy causes they support.

But the digitization of lotteries comes with a dark side: cybercrime. Lotteries have long had excellent and experienced security and IT teams, but the shift from physical security to cyber security requires new skills, expertise, and collaboration. With so many responsibilities and vendor systems to juggle, and how swiftly threats emerge, it can be difficult to stay attuned to all evolving risks and how rapidly they can negatively impact operations, profitability, and brand reputation.

Cybercrime has exploded over the past few years and the impacts are pervasive and significant. As threats grow in volume and complexity, lotteries face serious challenges in evolving and maintaining operational security. Lotteries are a tempting target, and a breach negatively impacts not only financial losses, but also threatens the lottery's reputation and damages player and stakeholder trust.

With so much at stake, proactive steps to manage risk, such as annual security testing to identify vulnerabilities and gaps before they can be exploited by cybercriminals are table stakes.

Our team is here to guide you. Senior lottery security experts like Gus Fritschie and his team have contributed to this eBook to give you a comprehensive look at the modern threats lotteries are experiencing with the rapid growth of technology, innovation, and cyber-attacks.

Gus Fritschie
Senior VP, Information
Security Services

Hopefully, this resource can guide your lottery in strengthening your defenses against modern cybercrime. If you'd like to connect, I am happy to discuss further – click here to connect with me on LinkedIn.

Steve Burns

ABOUT THE AUTHOR

Steve Burns, President & Chief Operating Officer, Bulletproof

As the founder of Bulletproof, Microsoft's 2021 Global Security Partner of the Year, Steve is passionate about helping businesses with their technology and security. With decades of experience, he is uniquely positioned to share his knowledge with business leaders who have varying levels of technical expertise.

Table of Contents

Chapter 1:
The Ever-Evolving Cybersecurity Landscape with Lotteries

In today's IT landscape, consumer behavior and adoption of a hybrid workplace model have greatly changed the way lotteries conduct business.

Cyberattacks have increased 400% since 2019 and cybercrime has become a global profit center. Global cybercrime costs are expected to reach $10.5 trillion USD annually by 2025 and a bad actor can easily get everything he needs to attack your lottery thanks to the cybercrime gig economy.

This, combined with the fact that many lotteries do not have robust cybersecurity plans or strategic roadmaps in place, means more gaps and vulnerabilities in lottery security exist.

The problem is amplified as a majority of lotteries do not have robust, managed security monitoring. This is critical to allow adversaries to quickly be detected, contained, and eradicated from computer networks before they can cause serious harm.

More Online Services = Bigger Risk for Lotteries

It's no secret that consumer habits and preferences have now predominantly shifted towards online services, and lotteries must keep up.

The adoption of cashless technologies, iLottery, and sports betting are great examples of how the industry has responded to consumer demand. But the ever-expanding cyber world means more potential vulnerabilities within your network that could pose challenges for clients and your workforce alike.

As the size of the attack footprint increases, it becomes more difficult to protect and secure your systems and applications alone.

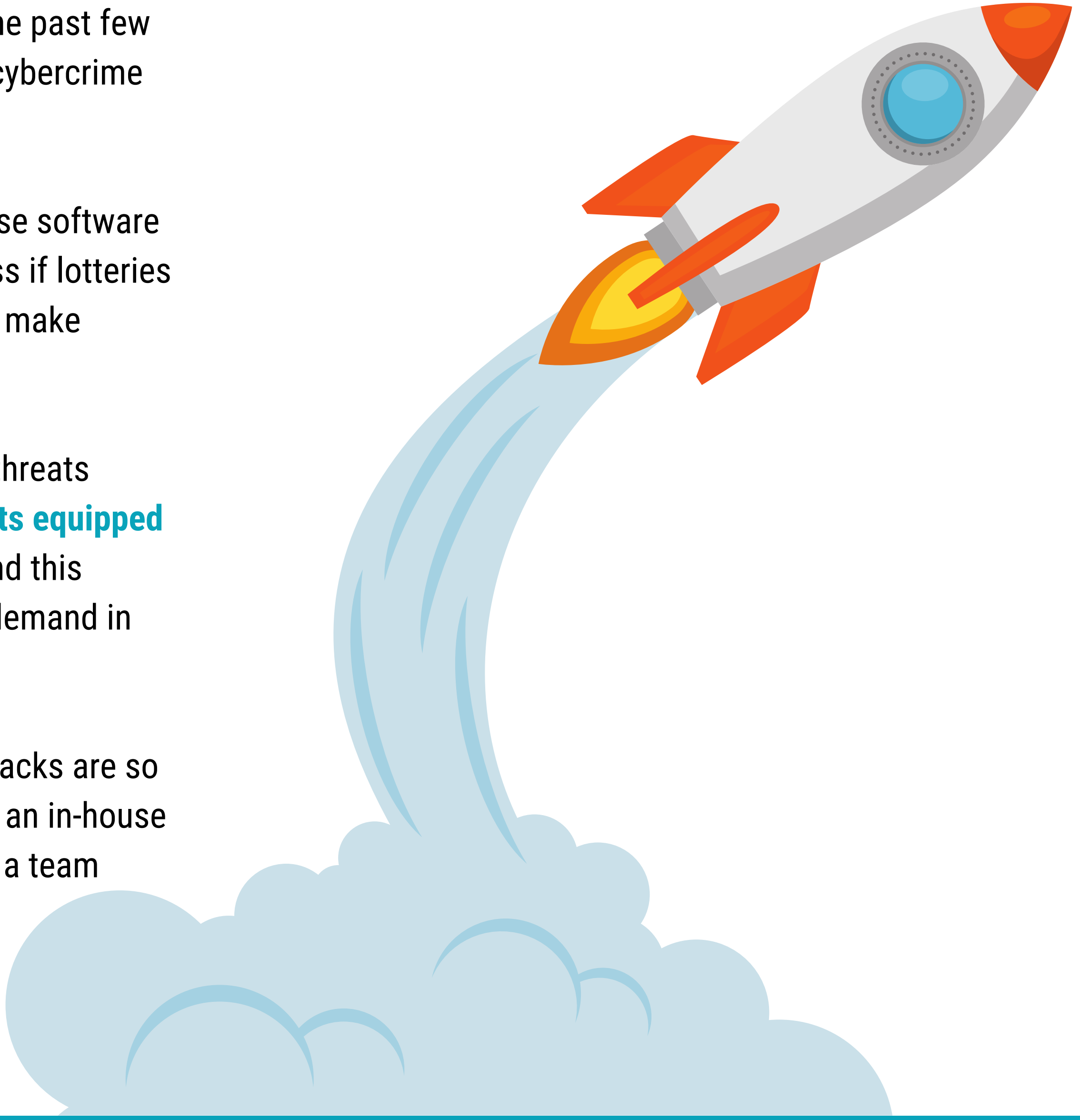
Why is Cybercrime Skyrocketing?

The complexity and frequency of cyberattacks have increased substantially over the past few years, and there's no sign of this growth slowing down. This is due to the thriving cybercrime gig economy.

Hacking software is now for sale, making it much too easy for amateurs to purchase software from expert cybercriminals. Not only that, the software virtually guarantees success if lotteries cybersecurity posture is not strong and robust for those looking for a quick way to make money.

For example, Ransomware-as-a-Service is one of the most pressing cybersecurity threats facing today's lottery industry. **Cybercriminals are now able to buy ransomware kits equipped with everything they need to be successful in their attack for just $66 upfront.** And this investment is just pennies compared to the potential return—the average ransom demand in 2022 was a whopping $400,000.

With this kind of malicious software so accessible to hackers, you can see why attacks are so common now. And not only that, they're also increasingly sophisticated. Even with an in-house IT team, you may not be able to prevent or respond to the harm in time. Security is a team sport, you need the right partners and vendors to help protect your lottery.



Key Challenges to Overcome

As the landscape continues to evolve, there are three key security challenges that lotteries face. Understanding these can help with devising a proactive plan to improve your security posture. We will explore these key challenges more in-depth throughout the eBook.

#1 Remote Workforce & Staffing

The pandemic exposed security gaps in many organizations including lotteries, due to quick remote work transitions that were necessary at the time. Many businesses jumped from using on-premise security and storage features to a cloud environment essentially overnight. Without any extra leeway to consider the most secure way to adapt to this setup, gaps were pretty much inevitable.

On top of an already fraught situation, there are security staffing shortages across the sector, posing more challenges to the industry as steps are taken to rectify these quick shifts.

#2 Acceleration of New Technology & Innovations

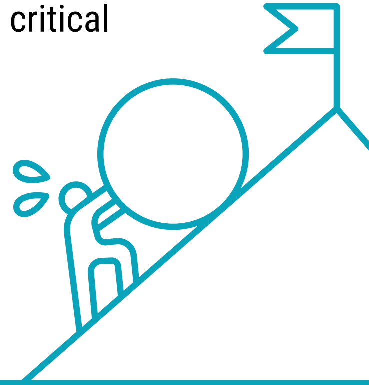
Lotteries have been resilient through change, however, tend to fall behind when it comes to adapting to new innovations timely compared to private-sector organizations.

New technologies expose new risks to account for. For example, it is projected that traditional on-premises systems will be shifting to the cloud sooner than later. Associations such as the Multi-State Lottery Association (MUSL) have specific guidelines for using the cloud which lotteries would need to consider. As new technologies continuously emerge, lotteries need to have a plan in place to ensure proper security protocols are met without falling behind.

#3 Third-Party Vendor Security

Lotteries rely on many third-party vendors for everything from operating their gaming systems to retailer management.

When this happens, lotteries need to ask questions such as how can the lottery gain assurance on the security controls of these vendors? What happens when they have a weakness or breach? Just how secure are these third-party vendors that we are leveraging? All critical questions to ask in the event a breach occurs.



Building Player Trust Is Essential For Lotteries

There's never been a more urgent time to consider a proactive approach to cybersecurity. But lotteries, in particular, must be diligent. With so much sensitive information being collected and stored through lottery games, apps, and wallets, it's vital to keep protected. If not, the confidence of your players is at stake.

For example: in February 2023, one NASPL Lottery was forced to contact 1,000 online players directly, asking them to change their passwords after detecting some "irregular activity." While the data breach was mitigated, the state agency said it was a "teaching moment." To maintain loyalty and trust, lotteries should avoid putting this burden on their players at all costs.

For instance, the information and money stored in a player's online account can also lead to security issues if not properly protected. To maintain their credibility, lotteries need to make their players feel comfortable with the products and games that they're playing.

Trust is essential. Lottery organizations are responsible for a lot of critical information—just what cybercriminals are looking for from vulnerable organizations. By prioritizing cybersecurity in an ongoing way, lotteries can build trust, and give consumers the confidence that both their data and funds are secure.

Chapter 2:
Planning Proper Protection & Compliance for Your Lottery

Governing bodies have a responsibility to ensure player data is protected, especially as cybercrime continues to soar. And with consumers top of mind, state and federal rules and regulations are constantly evolving, becoming more stringent.

The way regulations have been administered in the past doesn't match today's digital landscape, and it's often up to lotteries to take on the increasingly heavy burden of determining what regulations apply to their organization and trying to keep up.

For example, the World Lottery Association's Security Control Standard specifies required practices for security management. To remain compliant, organizations need to keep up with security requirements within lottery operations, technology suppliers, and multijurisdictional games.

As the industry continues to modernize, traditional on-premise systems like Random Number Generators (RNGs) and Internal Control Systems (ICS) are expected to move to the cloud as well.

With this in mind, it is imperative that lotteries take proactive measures. This can be done by ensuring their security protocols are up to par with guidelines, and even beyond compliance when possible. Getting ahead means reducing reactive efforts, as well as the associated resources and costs. If a lottery is constantly playing catch-up, they will find themselves vulnerable to security breaches and other IT issues that are likely to set them back.

Security compliance initiatives, such as WLA-SCS and ISO/IEC 27001 can be time-consuming, complex tasks which is why IT lottery teams often rely on trusted partners with industry experience to assist in these important projects.

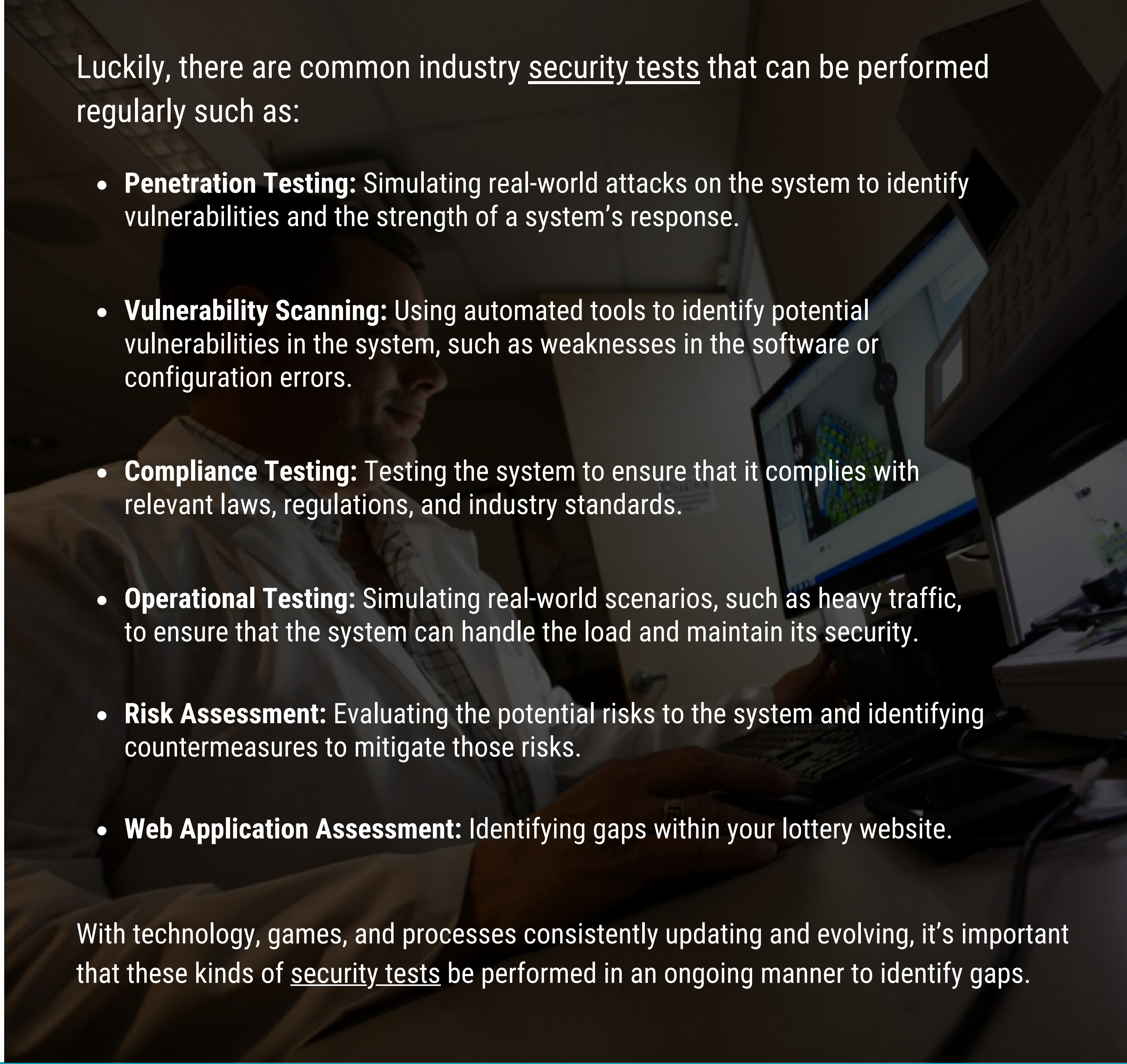
You Can Bet on Having Foresight

It's essential to take a proactive approach that goes beyond merely meeting compliance standards. By doing so, your lottery can be better prepared for new standards as they arise.

It also involves taking preemptive measures to address the vulnerabilities that hackers are highly skilled at identifying and exploiting.

This is key to protecting the lottery's reputation against loss of shareholders, customers, and public confidence.

It's clear why being proactive is the best course of action to stay secure. But how is this achieved? Anticipating and mitigating threats is an ongoing process.



Luckily, there are common industry security tests that can be performed regularly such as:

- **Penetration Testing:** Simulating real-world attacks on the system to identify vulnerabilities and the strength of a system's response.
- **Vulnerability Scanning:** Using automated tools to identify potential vulnerabilities in the system, such as weaknesses in the software or configuration errors.
- **Compliance Testing:** Testing the system to ensure that it complies with relevant laws, regulations, and industry standards.
- **Operational Testing:** Simulating real-world scenarios, such as heavy traffic, to ensure that the system can handle the load and maintain its security.
- **Risk Assessment:** Evaluating the potential risks to the system and identifying countermeasures to mitigate those risks.
- **Web Application Assessment:** Identifying gaps within your lottery website.

With technology, games, and processes consistently updating and evolving, it's important that these kinds of security tests be performed in an ongoing manner to identify gaps.

Lottery Security Solutions, Worth the Investment

It's critical for lotteries to investigate other solutions that would help to improve their security posture and stay ahead of the ever-changing IT landscape such as:

- **External/Internal Security Assessment:** Assessment to identify external/internal security gaps in your lottery network.
- **Web Server Security Assessment:** Test to evaluate if there are any vulnerabilities in your web server and how to remediate.
- **Lottery Security Audits:** Support various third-party security audits such as WLA Security Standard (WLA-SCS:2020), Internal Audit & Enterprise Risk Assessment, Lottery Source Code Security Audit, NIST CSF, etc.
- **Application Security for iLottery:** Security test of your lottery applications to identify gaps and areas of improvement.
- **Ransomware Threat Posture Assessment:** Proactive solution that enables lotteries to identify, assess, and mitigate risks associated with ransomware attacks.
- **Virtual Chief Information Security Officer (vCISO):** Get on-demand access to security executive who can help your lottery provide security direction to optimize your IT posture.
- **Security Program Development:** Evaluation of your security program and process, development/recommendations of programs that would help your lottery IT team (e.g., ADM Integrity Assurance Program).

Security Operations Center (SOC)

End-to-end security monitoring solution for lotteries

In today's world, with mobile workforces, volumes of connected users and devices, hybrid combinations of on-premise and cloud infrastructure, and a myriad of tools that don't communicate with each other, lottery IT teams face more demands than ever, often resulting in security gaps that leave you vulnerable. That's why it makes more financial sense to invest in a trusted security partner who can be there to provide end-to-end security services that will help your lottery:

- Reduce gaps in your lotteries' IT security
- Provide peace of mind, our experts will keep you protected and informed
- Provide 24/7 Security Incident Triage, Investigation, & Response
- Provide Advanced Threat Hunting
- Provide your employees with security aware training
- Allow your IT department to focus on activities that drive greater value

BULLETPROOF 365E ENTERPRISE

LEARN MORE

Microsoft Partner
Microsoft

2021 Partner of the Year Winner
Security Award

Prevent Disaster with Employee Security Awareness

Mistakes happen, but many security-related mistakes can be prevented. According to Verizon's 2022 Data Breach Investigation Report, about **82% of data breaches involve some kind of human error.**

Hybrid and remote work environments mean that staff are increasingly met with malicious links or email attachments, suspicious requests, malicious websites, and more. In-house IT staff are also overloaded and burnt out. Oversights are likely, even when an organization may appear buttoned down.

For example, Washington D.C.'s health insurance exchange experienced a data breach in April 2023. Thousands of users, including members of Congress, had their social insurance numbers and contact information leaked. This data was unfortunately stolen due to a security flaw that occurred from human error.

Security systems are only as good as the people who use them. So as a rule, staff education is crucial. Offering practical training to your employees can help fill in gaps that can drain resources, such as inefficient use of software. This approach can help educate against bad habits and give staff the go-to answers they need to maintain cyber safety on their devices.

Reducing Cyber Risks And Gaining Peace of Mind in Today's Market

Undoubtedly, there is a lot to account for when it comes to preventing cyber threats in lottery and gaming. From software updates to audit resources, and insurance to IT staff, the nuts and bolts of security protection can add up.

Investment in cyber insurance is one of a number of coordinated protective measures taken by organizations. In fact, this type of insurance is intended as a financial backup because it could cover costs arising from cyber-attacks.

While this is a reassuring option to have in your toolkit, these insurance premiums are at an all-time high due to the current rates of cybercrime. With the risk being so high, insurance companies need their prices to reflect what they could likely be paying out.

Organizations that invest in cyber insurance and proactive security controls and monitoring will get more peace of mind knowing they are covered. It's critical to take stock of your lottery security and identify ways to mitigate cyber risks since they can reduce insurance premiums, as well as the likelihood of an attack in the first place.

DID YOU KNOW?

Cyber insurance helps organizations offset the costs associated with responding and recovering from cyberattacks.

The growing frequency of cyberattacks has resulted in a spike in businesses opting for cyber insurance coverage from **26% in 2016 to 47% in 2020**.

The Challenges of Finding IT Talent, Globally

There is an extra challenge standing in the way of tightening up security measures—hiring IT staff.

Finding in-house IT staff is a particularly difficult task in today's market. Like many other industries, lotteries are struggling to find (and keep) talent. According to the 2022 Tech Salary Guide, 70% of all businesses are having a difficult time finding [IT] candidates with the right skill sets. And if you do manage to find the right talent, it is easy for them to become completely overburdened with responsibilities.

For organizations in a reactive state with limited hiring resources, small IT teams tend to spend their days putting out fires rather than preventing them. This quickly leads to burnout for the employees, which can lead to costly mistakes and/or resignation. Reactive IT is not a viable use of resources either. That's why gaming & lottery organizations are turning to Managed Security Services providers to help them outsource their security, ensuring ongoing security threat management and monitoring.

Given the IT staffing difficulty, lotteries face a significant challenge in growing their operations and keeping up with the ever-evolving digital landscape. A well-planned, sustainable approach is necessary to ensure the long-term stability of lottery operations. In the next chapter, we will explore some strategies to overcome these challenges and achieve success.

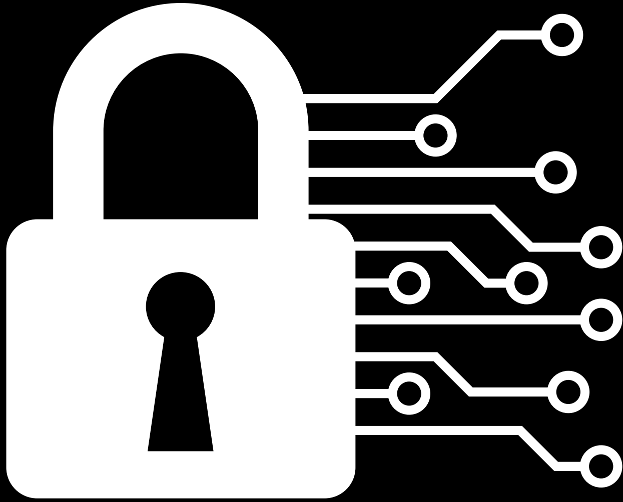
70% of all businesses are having a difficult time finding IT candidates with the right skill sets.

What are some key steps you can take as a lottery leader?

✓ **Be proactive –** Instill the importance of cybersecurity in your company culture, regularly schedule comprehensive security testing, and develop a strategic roadmap to set a path to success. The best way to minimize future risk is to act strategically in the present. Invest in your team and the resources that will ensure your lottery continues to fulfill its mission.

✓ **Collaborate with other industry leaders –** Develop your network and build new connections with industry leaders and peers. They are your best resources for understanding the lottery's cybersecurity landscape, including challenges, trends, regulatory developments, etc.

✓ **Don't be afraid to ask for help –** Reaching out for expert guidance and support is not a sign of weakness, but of strength and growth. Cybersecurity is evolving rapidly, and it's simply not possible for any lottery's internal team to keep up with everything. Seeking outside support will help ensure your lottery plans and technology roadmap is set up for success from start to finish.



☎ CONTACT US

Contact us today to learn how your lottery can benefit from partnering with us.

BULLETPROOF
a GLI® company

Sources

Cost of a Data Breach Report 2021 - 2023, IBM

Tech Salary Guide 2022 + Tech Issues Explained: The Cybersecurity Skills Gap by Microsoft

https://content.bulletproofsi.com/evolving_lottery_evolving_risk

https://gaminglabs.com/blog/security-is-the-key-to-future-lottery-success/

https://hired.com/state-of-tech-salaries/2022/

https://www.computerworld.com/article/3542681/how-many-jobs-are-available-in-technology.html

https://www.firewalltechnical.com/the-risks-of-hiring-an-in-house-it-support-department/

https://www.cyberstates.org/

https://www.linkedin.com/pulse/tech-issues-explained-cybersecurity-skills-gap-/

https://content.bulletproofsi.com/ebook-a-perfect-cybercrime-storm