
CALIFORNIA GAMBLING CONTROL COMMISSION

**GAMING POLICY ADVISORY
COMMITTEE PRESENTS:
CYBERSECURITY EDUCATION
RESOURCE GUIDE**



November 2025

Cybersecurity in Gambling Establishments

The Gaming Policy Advisory Committee (GPAC) met through 2024 and 2025 to discuss how to protect gambling operations, the reputation of the gambling industry in the state, and the health and safety of the people of and visitors to the state of California from cyberattacks.

As a result of those discussions, GPAC developed this Cybersecurity Education Resource Guide. This educational resource is being sent out to the cardroom industry in California to provide licensees with guidance on cybersecurity infrastructure recommendations and best practices.

If you have any questions about this cybersecurity educational resource or any other GPAC project, please email gpac@cgcc.ca.gov.

Cyberattacks on gambling companies have increased at an alarming rate in the past few years. Tribal casinos, commercial casinos, and gaming vendors have all been successfully targeted in cyberattacks, causing the release of private information, shutting down of gaming systems, and the targets paying ransoms to end the cyberattack.

These attacks have not been isolated to smaller operations with limited resources, as evidenced by the MGM cyberattack in Las Vegas in 2023, which ended up costing MGM Resorts over \$100 million.

An effective cybersecurity strategy protects not only sensitive information, but also safeguards reputation and builds trust with customers. By conducting regular reviews, gaming operators can identify potential vulnerabilities, ensure compliance with prevailing standards, and stay one step ahead of potential threats.

Taking proactive steps now can help mitigate future risks and avoid costly security breaches.

While this resource is strictly advisory and educational, GPAC hopes that all licensees take this guidance to heart as a part of a comprehensive cybersecurity strategy to protect themselves and the public from cyberattacks.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the Commission, and such reference shall not be used for advertising or product endorsement purposes. Named solutions providers are intended as a starting point and not a comprehensive and exhaustive list; pricing and offerings may vary.

Cybersecurity For All Cardrooms

As part of a comprehensive review of your cybersecurity structure, GPAC suggests that all gambling operations should do the following:

- Assess the security of your network and systems.
- Ensure employees are trained on current cyber threats and best practices.
- Update your software, applications, and firewalls regularly.
- Backup your data and have a disaster recovery plan in place.
- Consider consulting with cybersecurity experts for an audit or advice.
- Change email passwords regularly.
- Use MFA (multi factor authentication) for email and sensitive systems.
- Use anti-virus software and internet firewalls
- Keep customer information and your financial information on separate computers/systems that do not have internet access.
- Purchase Cybersecurity and Cyber Crime Insurance.

Cybersecurity for Medium-to-Large Cardrooms

GPAC suggests that medium-to-large gaming operations consider the following suggestions when assessing their cybersecurity systems:

Strong Password Policies

A strong password policy is essential for protecting a company's data and systems.

Regular Software and Operation Systems Updates

Keeping software and operating systems up to date is essential for protecting a company from cyber threats.

Multi-Factor Authentication (MFA)

MFA is a crucial security measure that significantly reduces the risk of unauthorized access by requiring multiple verification methods before granting access to sensitive accounts and systems.

Solutions Providers: Duo Security/Okta/LastPass



Secure Virtual Private Network (VPN) for Remote Access

A VPN is essential for securing remote access to company resources, protecting data from cyber threats, and ensuring encrypted communication over the internet.

Solutions Providers: Check Point/Palo Alto Networks/Fortinet

Next Generation Firewall Protection

A firewall is a critical security component that helps protect your company's network from unauthorized access, malware, and cyber threats.

Solutions Providers: Check Point/Palo Alto Networks/Fortinet

Antivirus Endpoint Detection and Response (EDR) Software

Antivirus and EDR solutions are crucial for protecting endpoints (computers, servers, mobile devices) against cyber threats such as malware, ransomware, and zero-day attacks.

Solutions Providers: SentinelOne/CrowdStrike/Microsoft

Data Backup

A robust data backup strategy ensures business continuity and protects against data loss from cyberattacks, hardware failures, human errors, or natural disasters.

Solutions Providers: Veeam/Acronis/Arcserve.

Regular Security Awareness Training for Employees

Security awareness training is essential for protecting your business from cyber threats, as employees are often the first line of defense against phishing, malware, and social engineering attacks.

Solutions Providers: CyberReady/KnowBe4/TitanHQ

Email Filtering to detect phishing and spam

Email filtering is a crucial defense against phishing attacks, malware, and spam that can compromise your business. Implementing a robust email security strategy will help prevent threats from reaching employees.

Solutions Providers: TitanHQ/Barracuda/Microsoft





Network Segmentation

Network segmentation is a cybersecurity practice that involves dividing a computer network into smaller, distinct segments or sub-networks to enhance security, performance, and manageability. By isolating different parts of the network, organizations can reduce the attack surface, limit the spread of security breaches, and improve overall network performance.

Incident Response Plan

An Incident Response Plan is essential for effectively managing and mitigating cybersecurity incidents.

Enhancing Endpoint Security with Managed Detection and Response (MDR)

MDR solutions are a critical component of modern cybersecurity strategies, particularly for enhancing endpoint security. MDR services provide organizations with advanced threat detection, response capabilities, and ongoing monitoring to protect against sophisticated cyber threats targeting endpoints.

Solutions Provider: SentinelOne/CrowdStrike/Microsoft

Intrusion Detection and Prevention Systems (IDPS)

IDPS are critical components of network security that monitor network traffic for suspicious activity and potential threats. They play a vital role in identifying and responding to attacks in real time, helping organizations safeguard their networks and data.

Solution Provider: Darktrace/McAfee/Palo Alto Networks

Third-Party Risk Management (TPRM)

TPRM is the process of identifying, assessing, and mitigating risks associated with third-party vendors, suppliers, and partners. Given the increasing reliance on external entities, effective TPRM is essential for safeguarding sensitive data, maintaining compliance, and ensuring business continuity.

Solution Provider: 1Exiger/RiskProfiler





Security Information and Event Management (SIEM)

SIEM is a comprehensive solution that aggregates, analyzes, and correlates security data from various sources to provide real-time visibility into an organization's security posture. SIEM plays a crucial role in detecting, responding to, and managing security incidents effectively.

Solution Provider: Splunk/CrowStrike/SolarWinds

Cybersecurity Governance Framework

A robust cybersecurity governance framework is essential for ensuring effective risk management, compliance, and overall cybersecurity posture within an organization. It provides a structured approach to managing cybersecurity risks, aligning security initiatives with business objectives, and fostering a culture of security awareness.

Solution Provider: Splunk/Vanta/NICCS

Identity and Access Management (IAM)

IAM is a critical cybersecurity discipline that focuses on ensuring that the right individuals have appropriate access to technology resources while maintaining security and compliance. IAM encompasses policies, processes, and technologies used to manage digital identities and control access to systems, applications, and data.

Solution Provider: Ping Identity/Okta/Microsoft



Additional Resources

[Small Business Administration — Strengthen Your Cybersecurity](#)

[Compliance Seminars — Cybersecurity for Small Businesses](#)

[National Cyber Security Alliance — Stay Safe Online Video Series](#)

[Amazon — Cybersecurity Awareness Training](#)

[UNLV Gaming Research and Review Journal — ‘High-Stakes’ Security: Current and Emerging Trends in Casino Gaming Cybersecurity](#)

