FIELD SERVICES

Protecting You from Security Threats Before They Start

BULLETPROOF
a GLI company

FIELD SERVICES

Go Beyond the Surface

The most dangerous assumption casino operators and regulators can make is that their computer systems are secure. However, security threats can come at any time, from both inside and outside of your casino. Most people only think of hackers when security incidents, such as outside breaches occur, but statistics show threats are more likely to come from within your organization. Gaming Laboratories International's (GLI®) Bulletproof division offers network risk assessments, system inspections, and software audits to help identify threats and reduce risk before it is too late.

NETWORK RISK ASSESSMENT

Mitigate Your Risk

Network Risk Assessments can help identify network security risks caused by common software vulnerabilities exploited both externally and internally by threats that exist anonymously on the Internet or from trusted staff. This service differs from regulatory compliance audits, such as PCI-DSS, because it is usually focused on specific criteria and ignores a holistic and comprehensive approach to security management.

Limit Unnecessary Exposure

Any device connected to the network can be vulnerable, which may include, but is not limited to, backup storage, multi-function printers, network servers, and smartphones. GLI will verify your operation's security by exposing weaknesses through actual hack attacks, ensuring your network controls work enterprise-wide. Based on their findings, our team of experts will recommend solutions to mitigate your risk.

After performing numerous network risk assessments at casinos, our experience has identified the following common vulnerabilities that expose you to risk:

- Poorly executed wireless security
- Un-patched domain controllers
- Poorly protected databases
- Unsecured web services
- Unprotected security cameras

Manipulation of Vulnerabilities

So, what does this mean to you? Everything. Manipulation of vulnerabilities can allow a hacker to exploit your systems and compromise your data in many different ways, including:

- Theft of personal information (e.g., driver's license or patron player account information)
- Manipulation of player points data
- Control of security camera systems
- Control of network systems
- Compromised integrity of email systems
- Compromised integrity of human resources data

WHAT HAPPENS DURING A NETWORK RISK ASSESSMENT?

Understanding the Checks and Balances

GLI will check all patron-accessible and back-of-house areas for open and live network jacks, as well as poorly protected wireless access points. We will attempt to gain access to casino assets using a combination of freeware, commercial tools, and techniques to evaluate your network, gaining a clear picture of the potential network risks your casino faces, including:

- External network architecture for a potential improper firewall and router configuration
- Weak authentication mechanisms
- Improperly configured database servers
- Vulnerable fileservers
- Simple Network Management Protocol (SNMP) checks
- Improperly configured or vulnerable email and Domain Name Server (DNS)
- Vulnerable IP-based security cameras
- Unprotected human resource data
- Missing vendor patches

A report detailing any discovered vulnerabilities and recommendations for preventing future difficulties will be generated.

NETWORK RISK ASSESSMENT

Identifying Threats Before They Happen

System inspections verify that the controlled files found in a particular system match those that have been previously tested by an independent third-party laboratory and comply with a particular jurisdictional standard or set of standards. Files are deemed "controlled" after analyzing the functions of those files with the participation of the system manufacturer. Controlled files are then given a unique signature which stays with the particular file version. Using the same tools that were originally used to create the signature, the signature is generated on-site where the online system is in use.

Keeping the Game Honest

If the generated signature varies from the certification letter, then either the files contain a different version than stated in the certification letter, or the files have been altered in some fashion. If it has been altered, then the files are deemed "uncertified." Depending on the function of the files, uncertified files could jeopardize the integrity of the system. If all files match the certification letter(s), we can certify that the system has been tested in one of GLI's labs.

COMMUNICATION TESTING

Making Sure the Game Is What It Is

No one pulls the wool over our eyes. Our professionals are trained to identify shady activity throughout the game deployment life cycle from start to finish. Communication testing is conducted on the casino floor to ensure gaming machines are communicating the metering information correctly. At the same time, this testing also checks to make sure the system is recording information correctly.

We Can See the Differences

GLI field inspectors verify the bill-in, ticket-in/ticket-out (TITO), and credits given (at the machine only) for each machine tested. The testing will either be the entire floor or a sampling of games on the floor and will generally include all manufacturers, different locations, and different currency denominations. This information is compared to the online system in order to ensure all records were passed through and logged in the system correctly. Our testing professionals make sure each game does what it is supposed to do.

If there is a discrepancy, the gaming machine or machines are retested for accuracy, and if the machine fails a second time, the gaming machine and the online system will be analyzed for discrepancies. This information is passed to governing agents for further review.

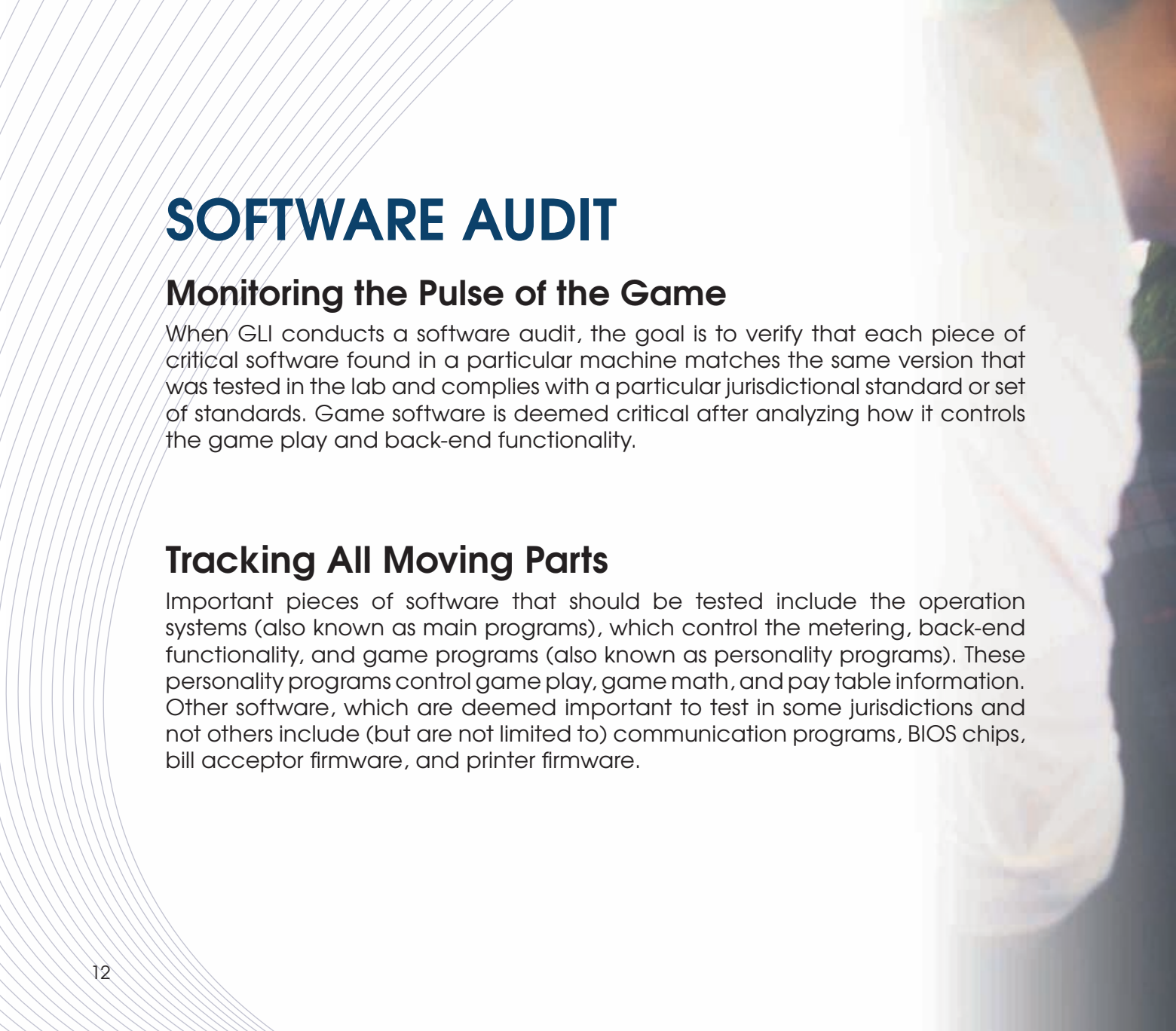
SOFTWARE AUDIT

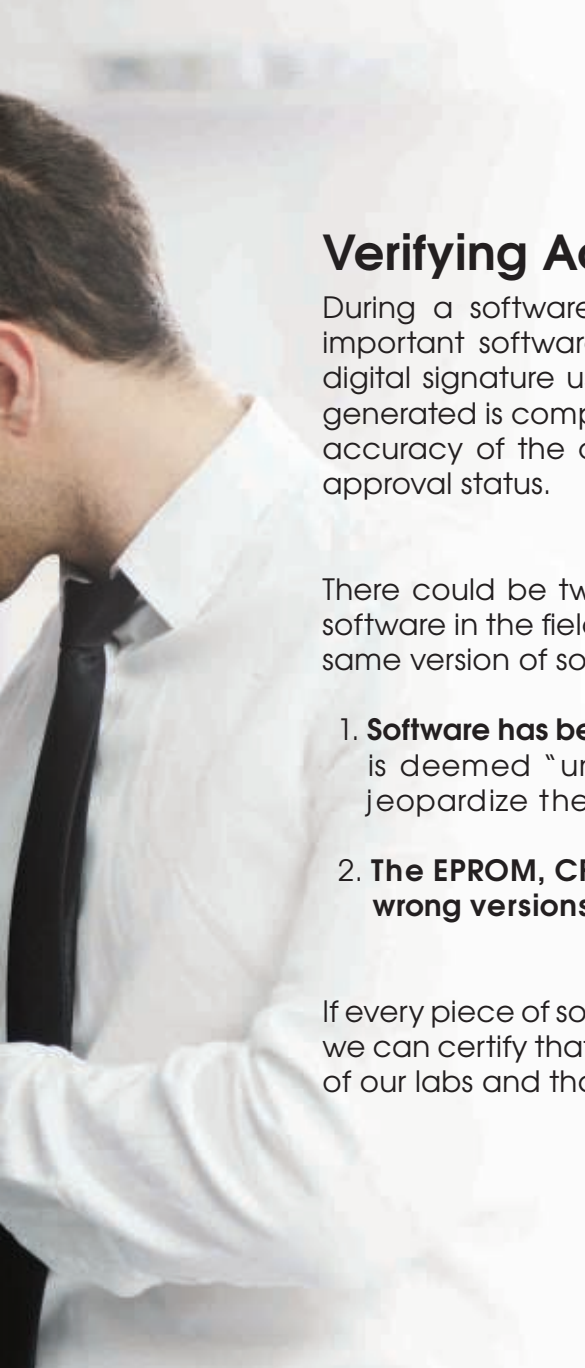
Monitoring the Pulse of the Game

When GLI conducts a software audit, the goal is to verify that each piece of critical software found in a particular machine matches the same version that was tested in the lab and complies with a particular jurisdictional standard or set of standards. Game software is deemed critical after analyzing how it controls the game play and back-end functionality.

Tracking All Moving Parts

Important pieces of software that should be tested include the operation systems (also known as main programs), which control the metering, back-end functionality, and game programs (also known as personality programs). These personality programs control game play, game math, and pay table information. Other software, which are deemed important to test in some jurisdictions and not others include (but are not limited to) communication programs, BIOS chips, bill acceptor firmware, and printer firmware.





Verifying Accuracy

During a software audit, GLI works with casino personnel to extract important software from each gaming machine and verify its unique digital signature using third-party verification tools. The signature that is generated is compared to GLI's extensive database in order to verify the accuracy of the digital signature and to obtain the software's current approval status.

There could be two reasons why a signature generated on a piece of software in the field does not match what is listed in our database for the same version of software:

1. **Software has been corrupted or altered.** If this is the case, the software is deemed "unapproved," and, depending on its function, could jeopardize the integrity of the electronic gaming machine (EGM).

2. **The EPROM, CF card, or other media that was verified contains the wrong versions of software,** thus generating an inaccurate signature.

If every piece of software that is audited matches what is in our database, we can certify that the EGM and all of its software has been tested in one of our labs and that the software has been verified.

SERVER-BASED GAMING INSPECTION

Downloadable Content, Player-Centric Technology, Skill-based Gaming, and Everything In Between

Server-based gaming inspections consist of investigating all servers and associated computer systems related on that particular closed Local Area Network (LAN). Only the functionality will be inspected. We will need the following information before performing a server-based gaming inspection:

- Game manufacturer type
- Specific version of software that is installed (or will be installed)
- Any computer systems on that specific network
- Number of games on the same network

Additionally, there will be communications testing performed on no less than ten games that communicate directly to the server.

SERVER INSPECTION

Optimizing Your Networked Floor

A server inspection consists of locating and obtaining a digital signature of the controlled files on the server(s). Manufacturers will apply policies on the server that will not allow additional files to be created and/or removed from the server itself.

FINAL REVIEW

BULLETPROOF
a GLI company

Ensuring Quality from Start to Finish

All information procured during the inspection will be collected for final review and an inspection letter with the findings will be sent to the requesting party. The requesting party will be responsible for furnishing the findings to all interested parties.

GLI is committed to helping your products and equipment stay safe and secure. For more information about Bulletproof field services, network testing, or network penetration testing, please contact your local Client Service Representative about network risk assessments.

GLOBAL LOCATIONS

GLI®

SO MUCH MORE THAN JUST TESTING

GAMING LABORATORIES INTERNATIONAL®

WORLD HEADQUARTERS
600 Airport Road
Lakewood, NJ 08701 USA
P: (732) 942-3999 • F: (732) 942-0043
gaminglabs.com

GLI's core purpose is to be the trusted global compliance and quality expert relied upon by our clients – delivering world-class customer service and value that is unmatched.