IDI
Billing Solutions

# Elevated Cyber Risks Demand Stronger Defenses.

## Is Your Business Ready?

IDI Billing Solutions

# Discover How Proactive Security Measures Can Safeguard Your Business in an Increasingly Complex Cyber Landscape

The importance of cybersecurity has never been more pronounced. In the last year alone, cyber threats have surged by nearly 30%, with businesses of all sizes finding themselves targets. The stakes are higher than ever, as data breaches, ransomware attacks, and other forms of cybercrime continue to evolve in complexity and frequency. According to a recent report from IBM and Ponemon, the average cost of a data breach in 2023 exceeded $4.4 million, a clear indicator that organizations must prioritize their cybersecurity strategies to protect their assets, customers, and reputation.

At IDI Billing Solutions, we understand the gravity of these threats. Our commitment to customer security is at the forefront of everything we do, and we've built a robust security program based on the National Institute of Standards and Technology (NIST) CyberSecurity Framework. This framework provides a structured and comprehensive approach to managing and mitigating cybersecurity risks, encompassing six key pillars: Govern, Identify, Protect, Detect, Respond, and Recover.


## GOVERN: Setting the Foundation for Robust Security Management

***The Govern pillar within the NIST CyberSecurity Framework establishes the foundation for an organization's cybersecurity risk management strategy. It involves setting clear expectations, defining roles and responsibilities, and ensuring continuous oversight of the cybersecurity strategy.***

Since our inception nearly 30 years ago, IDI has made security and trust a top priority. When we work with a prospective customer, security needs are always discussed early on. We have significantly invested in people, processes, and technology to ensure our customers' data is protected, and that our solutions are trusted and reliable. And as business needs, regulations, and risk management landscape change, we continue to enhance our security posture with an evolving and robust security program. It's an ever-changing process, and the job is never complete.

At IDI, we've identified and implemented robust security policies that govern all aspects of our SaaS platform and internal systems. Our governance model has been meticulously crafted over the years to align with industry standards and best practices. We maintain strict adherence to certifications and compliance frameworks, including SOC1/SSAE 18, SOC2 (Security, Availability, Processing Integrity, Confidentiality, and Privacy), PCI DSS, FIPS 140-2, and HIPAA. Regular checks, annual security assessments, disaster recovery drills, and detailed vendor evaluations ensure our governance model remains effective and aligned with evolving risks.

IDI Billing Solutions

## IDENTIFY: Understanding and Prioritizing Cybersecurity Risks

***The Identify pillar of the NIST framework focuses on understanding an organization's assets, suppliers, and associated risks. This understanding enables the prioritization of cybersecurity efforts in line with the organization's overall risk management strategy.***

At IDI, we take this principle to heart by conducting comprehensive information security risk assessments. Our Security and Risk Management team regularly evaluates the environment to identify potential vulnerabilities. This includes defining the frequency of checks, assigning responsibility, and developing actionable plans to mitigate identified risks. Our robust Third-Party Provider Management Policy ensures that all third-party vendor agreements are rigorously assessed for risk.

## PROTECT: Safeguarding Assets with Comprehensive Security Measures

***Once risks are identified, the Protect pillar emphasizes the implementation of safeguards to secure the organization's assets. This includes measures such as identity management, data security, platform security, and infrastructure resilience.***

To ensure customer protection, we have developed and implemented safeguards in three key categories to ensure delivery of critical infrastructure services:

### 1. Data Security Controls

Robust processes that include:

- Commercial-grade password manager
- Multi-factor authentication and just-in-time privilege escalation
- Secure coding reviews of all security-impacting changes
- Regular patching for all systems and applications
- Frequent Application and Network Penetration Testing
- Strict network segmentation and firewall rules

### 2. Physical Security

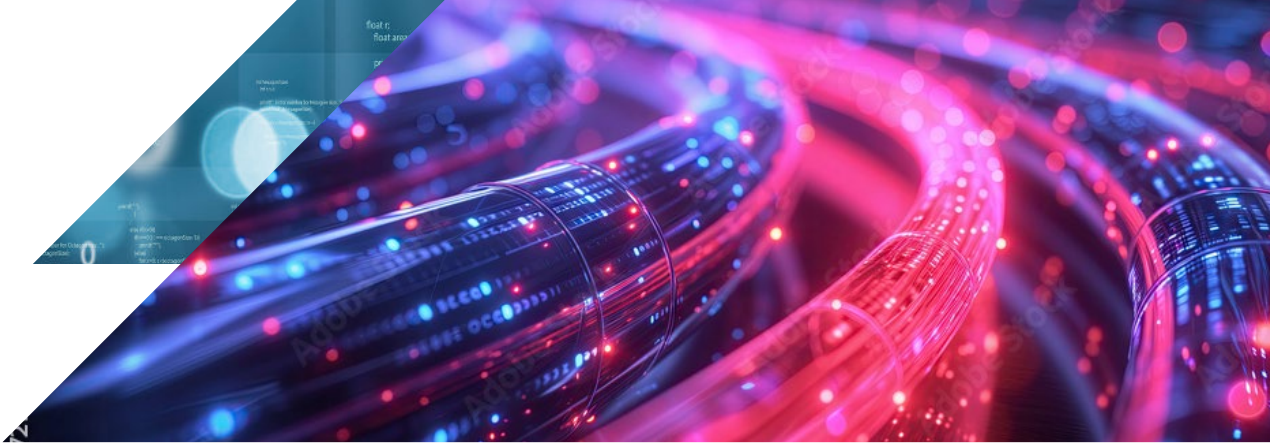
- Hardened facilities that include badges, guards, cameras, and comprehensive on- and off-boarding processes

### 3. Trusted People

Rigorous training and process checks to ensure total commitment to customer security, including:

- Secure coding reviews of all security-impacting changes
- Strong change management and configuration management processes
- Regular Security Monitoring of network & device traffic and event management
- Monthly phishing campaign tests

IDI Billing Solutions



## DETECT: Identifying and Analyzing Cybersecurity Threats

***The Detect pillar is crucial for the timely discovery and analysis of potential cybersecurity threats. This involves monitoring systems for anomalies and indicators of compromise that could signify an ongoing attack.***

We are relentless in our pursuit of continual monitoring and review, so that in the instance a cybersecurity event does occur, we're immediately aware. Implementations include:

- Network intrusion detection and prevention system
- Continuous security monitoring – network and device traffic; personnel activity
- Robust SIEM (Security Information and Event Management) processes and tools
- Regular scanning and review of assets and vulnerabilities of all security-impacting changes

## RESPOND: Taking Swift Action to Mitigate Cybersecurity Incidents

***When a cybersecurity incident is detected, the Respond pillar ensures that organizations can effectively contain and mitigate the impact. This involves incident management, communication, and analysis.***

In the instance a cybersecurity event does occur, the IDI team is poised to take immediate action through:

- Highly trained incident response team and well-designed response planning processes and procedures (including process drills and table-top exercises)
- Detailed forensics process – performance and analysis
- Robust mitigation and containment processes
- Continuous update of risk register based on lessons-learned

## RECOVER: Restoring Normal Operations After a Cybersecurity Incidents

***The Recover pillar focuses on restoring assets and operations affected by a cybersecurity incident. It emphasizes the importance of timely recovery to reduce the impact on the organization.***

IDI maintains plans for resilience — positioned to quickly restore any capabilities or services that are impaired due to a cybersecurity event through:

- Well-designed recovery planning procedures and regular recovery process drills
- Robust communication planning with key stakeholders
- Continuous optimization of processes based on lessons learned

IDI
Billing Solutions

## Turning Risk into Opportunity:
## IDI's Commitment to Adaptive Cybersecurity

As cyber threats continue to grow in both number and sophistication, the need for effective risk management has never been greater. At IDI, we recognize that the landscape of cybersecurity is constantly evolving, with hackers continually finding new ways to breach even the most secure environments. In response to these challenges, we remain resolute in our commitment to protecting both proprietary and customer data, reducing the likelihood and impact of potentially damaging compromises.

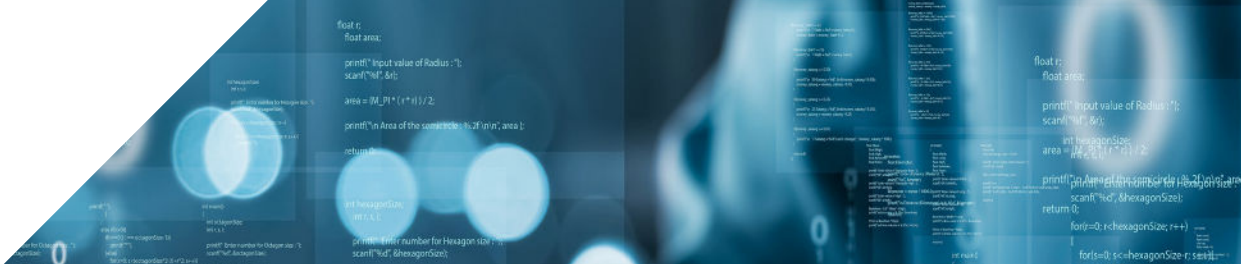
However, our approach to cybersecurity extends beyond just defense. While many cybersecurity risk management activities focus on preventing negative events, they can also create opportunities for positive outcomes. By implementing robust security measures, we not only safeguard our operations but also enhance our overall business performance. Strong cybersecurity practices can increase customer trust, improve operational efficiency, and even open new revenue streams. At IDI, we view cybersecurity as a strategic advantage, enabling us to capitalize on opportunities that come from a secure and resilient operating environment.

## Transform Cybersecurity Challenges Into Strategic Advantages.
## IDI Can Help.

In today's rapidly evolving threat landscape, cybersecurity is not just a necessity — it's a strategic imperative. At IDI, we've turned risk management into a proactive force that drives our business forward. Our comprehensive security program doesn't just protect; it enhances our operations, strengthens customer trust, and opens doors to new opportunities.

If you're ready to fortify your security posture and discover how robust cybersecurity can fuel your growth — or if you have questions or insights to share — we'd love to connect. Let's work together to secure your future.

Contact us at **800.200.6151** or schedule a consultation call at **idibilling.com/demo**.



## About IDI Billing Solutions

For nearly 30 years, IDI Billing Solutions has been a trailblazer in the telecom space — revolutionizing the industry through a world-class, cloud-based billing and operations support system (BSS/OSS). Designed to support innovative offerings, complex rating schemes, and diverse business models, IDI's robust platform delivers on our commitment by providing customers with the freedom and flexibility to enhance the digital experience, automate operations, expand services, and seamlessly scale as their business grows.

Through innovative technology, people, partners, and systems, we're dedicated to building a better experience for those we serve by providing advanced customer experience management technology, backed by proven best practices, relevant use cases, and comprehensive service, that telecoms need to stay ahead of the curve. At IDI, we are a guiding force — deeply committed to enabling our customers to deliver optimal digital experiences for their customers.

Resources


- National Security Agency (NSA) Cybersecurity Advisory: Protecting VSAT Communications
- NSA Cybersecurity Technical Report: Network Infrastructure Security Guidance
- Office of the Director of National Intelligence (ODNI): Annual Threat Assessment of the U.S. Intelligence Community, February 2022
- CISA Tip: Choosing and Protecting Passwords
- CISA Capacity Enhancement Guide: Implementing Strong Authentication
- What is HITRUST? A Comprehensive Guide, Richard Reiben (CISSP, PMP, CCSFP)
- Check Point Research (CPR) Q2 2024 Global Cyber Attacks
- IBM Cost of a Data Breach Report 2024