IT & DATA SECURITY PLATFORM FOR BUSINESS-CRITICAL COMMUNICATIONS

Where security drives compliance

Understand why over 1,500 businesses trust RRD with the secure delivery of financial, healthcare, insurance and transactional documents.

Hacking a server, installing malware, or influencing human behavior through a sc
— the nature of “threat actors'' has changed over the years. The proverbial bad g
past were individuals looking for personal financial gain or perhaps a claim to fa

Today's threat actors are motivated, organized criminals (usually with nation-sta
for whom this is a business. A business they are particularly proficient at.

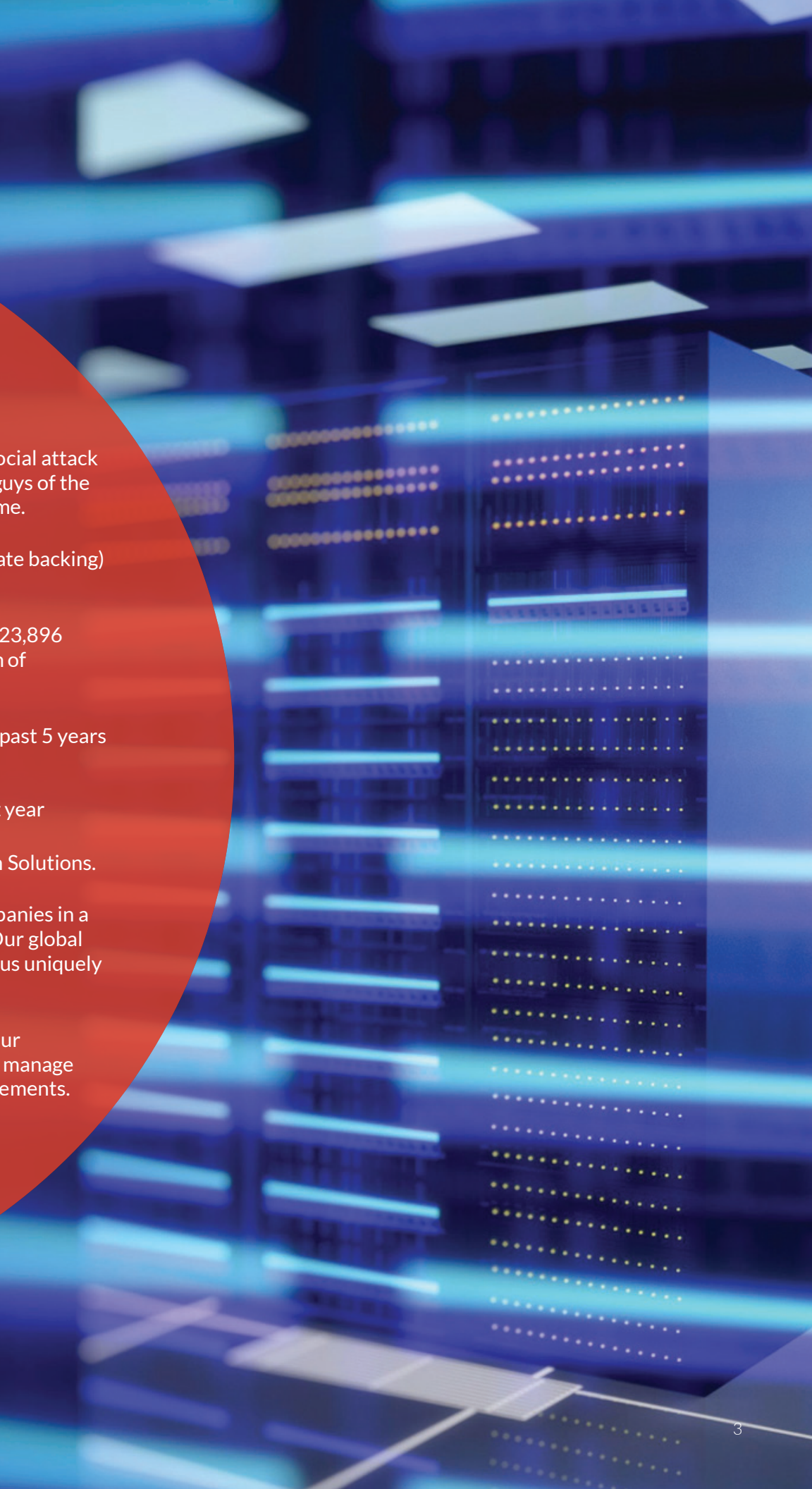
According to Verizon's 2022 Data Breach Investigation Report, which analyzed
reported security incidents at major companies (of which, 5,212 included breach
confidential data):

- YoY ransomware attacks increased by 13% — an increase greater than the
  combined
- Nearly 4 in 5 breaches can be attributed to organized crime.
- Human element was involved in 82% of all breaches analyzed over the past

Eye-opening statistics — and all reasons to talk to RRD Business Communication

Our comprehensive security offering is engineered to address the needs of comp
highly-regulated industry for the most demanding data security requirements. O
network of security experts, and meticulous data management approach makes
qualified to store and protect customer information.

Organizations reliant on transactional communications regularly turn to us for o
longstanding commitment to information security, proven ability to process and
highly sensitive data, and deep understanding of industry regulations and requir


ocial attack
guys of the
me.
ate backing)
23,896
n of
past 5 years
year
n Solutions.
panies in a
Our global
us uniquely
ur
manage
ements.

RRD's IT Security Platform for Business-Critical Communications

Clearly defined incident response measures

RRD's well-defined, documented and audited process addresses any incident as it occurs. Our staff is specifically trained in incident response to properly guide operations teams and engage appropriate external parties as necessary.

Rigorous and frequent third-party auditing

RRD's annual SOC2+HITRUST CSF report attests to RRD's compliance with HITRUST CSF controls and three of the AICPA Trust Services Criteria. We frequently test — which includes third party penetration testing of our networks and facilities — the practical effectiveness of the security controls we have in place.

Continuous systems monitoring and protection

RRD networks are designed and implemented with appropriate trust boundaries to control access to sensitive data. RRD's Security Operations Center (SOC) provides 24x7 monitoring of a wide variety of information from various platforms identifying and acting on potential security events.

We also routinely assess our systems and applications for vulnerabilities, adhering to strict patch management protocols.

Secure facilities, stringent standards

RRD only processes customer data in facilities approved to handle confidential and private information. These facilities feature physical security boundaries, strict access control features, and comprehensive protocols around sensitive assets. Facility employees must wear visible identification at all times and are monitored with video surveillance in production areas where private or confidential work is carried out. All systems access is granted on a least-privilege basis to confirm that staff has access only to data relevant to their job.

Leading technology, world-class service, peace of mind

RRD delivers solutions that are focused on disaster recovery, business continuity, and organizational resilience. From data center service partnerships to backup and failover environments at geographically dispersed locations, we deliver around-the-clock account service customized precisely to your needs.

Tailored approach to data security

RRD knows data and data security. By maintaining a comprehensive data governance and management program, we manage sensitive data throughout its lifecycle to ensure proper handling and disposal.

Rigorously-screened and highly-trained workforce

Our IT workforce spans the globe to accommodate your needs. All job applicants are carefully screened — particularly those applying for positions requiring access to private or confidential information.

Our application process includes thorough background checks and nondisclosure agreements detailing security and legal responsibilities. Once hired, team members receive ongoing job-specific training as well as security awareness training.

Comprehensive security and compliance

RRD has a dedicated security and compliance team managing and monitoring all security controls, audits, assessments and incidents. Our security and compliance program is built on the internationally recognized frameworks of NIST CSF and the three AICPA Trust Principles of Data Security, Data Confidentiality, and Data Availability.

Our framework also maps to specific healthcare and privacy regulatory legislation including but not limited to:

- Health Insurance Portability and Accountability Act (HIPAA)
- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- Payment Card Industry Data Security Standard (PCI DSS)
- ISO 27001

Premier Data Privacy Program

For any communications services organization, a focus on data privacy is equally as critical as a focus on data security and compliance. The depth, breadth, and consistency of RRD's security program is matched by its privacy program.

Our privacy program addresses a number of domestic and international privacy laws and regulations, including:

- EU General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA) — and other U.S. state privacy laws
- Chinese Personal Information Privacy Law (PIPL)
- Philippines Data Privacy Act

A global dedication to privacy

We maintain a global staff dedicated to managing our privacy obligations, including a Chief Privacy Officer, regional Privacy Managers, and in-house legal counsel with special knowledge on privacy regulations and concerns.

RRD also has ongoing relationships with external legal firms specializing in privacy matters. RRD is engaged with and is a corporate member of the International Association of Privacy Professionals (IAPP).

RRD's Global Incident Response Program is designed with the understanding that any adverse event involving sensitive customer data is likely to have security, regulatory, and privacy components and addresses all aspects with equal diligence.

In fact, RRD offers services to our customers to assist with data breach notifications procedures and communications resulting from data exposure incidents within their organizations.

For more information, contact the RRD Business Communication Solutions team today.

Where security drives compliance.
Visit **rrd.com/bcs**