Security

GEORGEJON

GEORGEJON.COM

George Jon is your guard dog.

As the global leader in eDiscovery platform design and management, George Jon deploys, oversees and secures mission-critical client environments for high-profile, high-risk industries around the world. Threats are ever-present and constantly evolving, but by leveraging George Jon's team of experts to assess the current security posture and/or provide 24/7 proactive security management of an eDiscovery environment, clients can feel safe and secure in their daily activities, knowing that their data-rich systems are protected and performing at peak capacity.

42%

Only 42% of companies attacked are able to fully recover their data from a backup

$50B

The yearly virus damage to US businesses is $50+ billion

300%

Due to demand and growing needs, GJ has increased its staff of Security Experts by 300%

GJ Security Services leverage a system of controls, cutting-edge products/tools, and best practices (developed and honed over 15 years of real-world experience) to ensure the perpetual integrity of client environments. With every deployment, we provide solutions that combat today's ever-evolving security threats, both internal and external. Moreover, our team of Security Engineers specializes in positioning client environments for the rigors of InfoSec audits, ensuring operational fidelity and peace of mind that allow you to focus on your core business.

We offer clients a comprehensive portfolio of security services, specific to the eDiscovery industry, that can be employed to confidently assess and manage all of the **Key Security Considerations**:

Security Components & Products

We work hand in hand with industry pioneers and tech leaders to bring clients proven solutions to critical security needs.

SONICWALL · braintrace · vmware · thycotic · Quest · TREND MICRO · SECURELINK · CITRIX · Qualys. · G360

Security Audits

Knowledge is power.

The George Jon Security Team will conduct an end-to-end security assessment of your environment and operating model, from planning to execution.

We will conduct on-site and virtual interviews, coupled with remote environment review sessions, to diagnose the current state of your security posture. This is followed by a gap analysis, relative to industry best practices, and recommendations for galvanizing your environment across the following parameters:

- Data workflow and data management, including the end-to-end data handling process, from acquisition through remediation
- Identity and access management solutions for optimization opportunities and gap/weaknesses identification in process and controls
- Vulnerability management, from scanning to remediation, aligned with business SLAs
- Encryption methodologies in conjunction with data workflow and management
- Security architecture relative to zone separation, perimeter controls, egress filtering, and proxy internet access
- Cybersecurity operations, response plans, and process effectiveness/preparedness
- Application security configurations and recommend baseline images for security enhancement

SECURITY AUDIT BENEFITS

Identifies weaknesses in your security posture that expose your business to unnecessary risk

Explains industry Best Practices and how other organizations in the eDiscovery realm are protecting their environments

Provides insight across security tools and controls, backed by GJ testing, that ensures efficacy while avoiding platform performance and stability degradation

Forges a clear and defined roadmap for achieving a “Desired State” environment security posture

Delivers an end-to-end overview of your current data handling and management workflow, identifying key areas for improvement

SECURITY AUDIT FRAMEWORK

Our solution framework for conducting and delivering successful client Security Audits consists of three holistic phases to ensure we not only capture and present an accurate representation of your current state, but also understand and construct a roadmap for achieving the ideal future state.

PHASE 1

GJ holds client workshops and gathers environment security documentation, conducting a 360-degree security review of the environment to determine the current baseline state.

Information Gathering
- Security vision and management expectations
- Current InfoSec policies and procedures
- Existing environment documentation
- Data workflow documentation
- Client-required information security controls

Assess and Baseline the Current State
- Security tools and configuration
- Cyber Ops and response plan
- Data handling and encryption
- Security-based environment pain points

PHASE 2

GJ compares the current state baseline against industry-specific security best practices to deliver a gap analysis across key security controls, prioritized by risk severity and expectations.

Gap Analysis
- Data encryption
- Identity and access management
- Vulnerability management and patching
- Security operations (SIEM)
- Security architecture
- Data handling

Prioritize Security Findings
- Alignment to management expectations
- Alignment to industry best practices
- Alignment to contractual requirements
- Budget considerations
- Implementation intensiveness (complexity, impact, tradeoffs)

PHASE 3

George Jon's Security Team will deliver a final Security Assessment Report & Executive Summary detailing key areas for risk mitigation and outlining the "Desired State".

Security Health Report and Remediation Roadmap
- A comprehensive view of the current state, identifying critical security weaknesses and the associated remediations
- Prioritization of security concerns and the associated risks aligned with management acceptance
- Detailed implementation plan broken down by workstream, with budgetary and timeline estimates

Password Protection

Save money. Save time. Save face.

Law firms, service providers, and corporations all over the world are under assault by sophisticated hackers looking to leverage the wealth and visibility of the legal world's data for illicit profit. They recognize that eDiscovery data is a valuable prize, as these mission-critical client data assets can be used to cripple reputations, profitable operations, and the ability to protect client information. The hackers demand significant ransom payments to prevent them from posting confidential client information online, which would destroy the reputation and financial stability of any law firm.

80%

In 2019, 80% of hacking-related breaches involved compromised or stolen credentials

58%

58% of companies are not able to fully recover their data from backups

In 2019, 80% of hacking-related breaches at law firms involved compromised or stolen credentials. As such, protecting access to your data systems is critical for revenue generation, daily billing operations, and the firm's professional integrity. Think about what can happen when you lose control of your systems:

- Your billing and timekeeping systems could be rendered inaccessible/inoperable, costing the firm millions in a single instance and permanently damaging your public reputation.
- Your eDiscovery software could become useless mid-production, forcing you to miss client- and court-mandated deadlines, costing the firm millions.
- You could be forced into the impossible situation of paying a ransom or suffering the release of client information and enduring permanent reputational harm.
- Insurance costs could skyrocket, an expensive proposition at a time when firms are working to cut overhead.
- You could permanently lose critical/confidential data — 58% of companies are not able to fully recover their data from backups.

Now is the time to reclaim control of your password-protected data assets and minimize the potential for employee/vendor malfeasance that can destroy credibility and profitability. George Jon offers law firms, service providers, and corporations a fresh start and peace of mind, employing 15 years of real-world experience to tactically address and remediate security risks. The service even provides you with a competitive advantage when pursuing new accounts, as you can tout the state-of-the-art data security systems you've implemented to prospects.

The Password Protection service eliminates risk associated with providing user-level access to database and service accounts (eDiscovery software, financial/case/document management systems) to employees/vendors. We provide a one-time reset of all critical passwords, vault the newly created passwords using our Identity and Access Management (IAM) software, and implement a dynamic password management system that rotates privileges after every approved use. Passwords are logged for auditing purposes, making them both trackable and impossible to compromise.

Once in place, the service provides proactive, ongoing management of privileged accounts to ensure security, eliminate the need for future password resets, and provide planned systems auditing and reporting for peace of mind. An added bonus: the service can help REDUCE your cyber and liability insurance costs, as most insurers require security measures as a precondition of coverage, and firms with proven security practices receive lower insurance rates.

Hackers cannot achieve their goal without access to your network. Protect both your employees and the firm from the possibility of compromised data systems – call the experts at George Jon today for a proposal to protect your kingdom. We've successfully implemented this security protocol for many of our AmLaw 100 and Service Provider clients, and look forward to helping you secure your valuable data.

Security as a Service

InfoSec without insomnia.

In industries across the business world, data platform security and protection is a costly and resource-intensive endeavor. In the eDiscovery realm, security and protection are mission-critical functions, as collected data is highly confidential, centralized, and a target for malefactors. Further complicating effective security management is that many security tools and controls can have a devastating impact on the performance and stability of eDiscovery environments due to the burst or surge amounts of data transmission, potentially resulting in dissatisfied clients and missed production deadlines.

Over the past 15 years, George Jon has worked hand in hand with our global pool of eDiscovery clients to balance security, performance, and cost initiatives relating to information security requirements and escalating/evolving user demands. After spending thousands of hours of researching, testing, implementing, and configuring security tools and controls, we have developed a holistic security management program that leverages state-of-the-art controls, industry-leading resources, and proven best practices to ensure the integrity and performance of client environments. And we can provide optimized outcomes at a fraction of cost of users trying to achieve success by themselves.

KEY TENETS OF SECURITY AS A SERVICE

IDENTITY & ACCESS MANAGEMENT

- Privileged access management (role-based access control)
- Password vaulting and rotation
- Multi-factor authentication
- Access audit and logging
- Single sign-on

VULNERABILITY MANAGEMENT

- Continuous vulnerability scanning across platform software systems
- Prioritized vulnerability patching, based on severity
- Ongoing vulnerability reporting and environment certificate monitoring

DATA ENCRYPTION

- Database Encryption – SQL TDE
- TLS 1.2 and SSL Certs for in-transit data
- Physical disk encryption for SAN natives
- vSphere encryption
- BYOK

APPLICATION HARDENING

(SECURITY BASELINE IMAGES)

- Relativity
- Nuix
- Brainspace
- Ipro

SECURITY ARCHITECTURE & CONTROLS

- Zone separation by tier
- Standardized, consistent use of IDS/IPS
- Traffic communication control
- Egress filtering and proxy internet access
- Change management, asset inventory tracking
- Data segregation

SIEM & SOC (OPTIONAL)

- Threat monitoring and alerting
- Threat hunting and pivoting
- Security log review
- Event correlation and retention