Cybersecurity & Privacy

INNOVATE. TRANSFORM. SUCCEED
Adapt to the new business reality.

protiviti
Face the Future with Confidence
How well is your organization adapting to the ever-changing demands of today’s marketplace? Implementing the right mix of technology and programs to innovate, protect margins and build shareholder value while keeping your data assets safe requires a partner that can help you succeed. Trust Protiviti. We’ll help you find the right solutions to make your business excel.
Protiviti provides consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 85+ offices in over 25 countries

- Serve 60% of Fortune 1000®
- Serve 35% of Fortune Global 500®
- We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.
- Protiviti is a subsidiary of Robert Half International

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

We leverage emerging technologies and methodologies to innovate, while helping organizations transform and succeed by focusing on business value.

Our advanced solutions range from strategy development through design, implementation and managed services. We are also experts in operational resilience, data and analytics, cybersecurity and privacy, cloud, application implementation, artificial intelligence and robotic process automation.

See why Protiviti is the right choice to innovate, transform and succeed.
Technology Strategy and Operations
- Business Transformation & Strategy
- Technology Strategy
- Technology Services Delivery
- Technology Risk Management & Governance
- Transformation Program Execution

Cybersecurity and Privacy
- Security Program and Strategy
- Data Privacy and Data Security
- Attack and Penetration
- Incident Response and Cyber Resilience

Digital Identity Services
- Strategy and Advisory Services
- Digital Identity Integration and Sustainment

Cloud Solutions
- Strategy and Governance
- Transformation and Modernization
- Cloud Migration
- Cloud Security

Enterprise Application Solutions
- Solution Design and Selection
- Implementation Services
- Application Security and Controls

Software Services
- Custom Business Applications
- Cloud Applications
- Website Design and Solutions
- Intelligent Automation Enablement
- On-Demand Services
- GRC Solution Implementation

Enterprise Data and Analytics
- Enterprise Data Governance
- Enterprise Information Management
- Reporting and Visualization
- Software and Digital Strategy
- Business Strategy and Advanced Analytics

Emerging Technology Solutions
- Strategy, Design, and Business Case Identification
- Prototype/POC
- Implementation, Management and Support

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
We have flexibility to tailor our delivery models to meet your organizational needs:

<table>
<thead>
<tr>
<th>BLENDED DELIVERY</th>
<th>ONSHORE DELIVERY</th>
<th>OFFSHORE DELIVERY</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Project leadership delivered in collaboration with skilled resources</td>
<td>• Delivered in collaboration with our consulting solution centers</td>
<td>• Delivered in collaboration with our offshore solution centers</td>
</tr>
<tr>
<td>• Local, specialized talent with option to convert to permanent</td>
<td>• Access to Robert Half’s 24x7 Service Center with Tier 1 and 2 technical and operational support staff</td>
<td>• Greater concentration of resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reliable, optimized source of talent</td>
</tr>
</tbody>
</table>
MANAGED SOLUTIONS VALUE

**OUR MANAGED SOLUTIONS PROVIDE YOU WITH**
- Cost reductions by avoiding over hiring
- Bandwidth to prevent burdening full-time employees to deliver on projects
- Ability to scale up or down as needed
- Experienced subject matter experts, on demand, for unique and complex issue

**ADVISORY**
Identify, anticipate and solve problems through transformation and implementation
- Solving complex programs with Agile methodologies and design thinking while managing deliverables, milestones and outcomes
- Technology enablement through artificial intelligence, machine learning, process mining and robotic process automation

**SEAMLESS OPERATION**
Manage or fix functions, processes or data to free up your team to work on what matters
- Cost efficiencies: Flexibility to scale up or down with the right resources at the right time (onshore or offshore)
- Reduced risk: Performance, productivity and service levels are our responsibility

**THE RIGHT TEAM**
Address skillset gaps and hiring challenges
- Maintaining control and oversight of the resources
- Access to specific, specialized skills and expertise that cannot be found on your internal team
- Time saved to upskill your existing team
OUR DELIVERY CENTER CAPABILITIES

Protiviti India Member Firm
- IT Audit and SOX & Financial Controls
- Risk and Compliance
- Business Process Improvement
- Security and Privacy
- Enterprise Data & Analytics
- Enterprise Application Solutions
- Managed Services

Protiviti Capability Center (India)
- Software Development
- Package Tools Implementation
- Enterprise Content Management
- Knowledge Management
- Research and Analytics

Las Vegas Service Center (RH)
- Managed Help Desk
- IT Infrastructure Support
- IT Monitoring and Incident Response
- IT Hardware Deployment
- IT SOP Documentation and Execution

Protiviti India Member Firm
- Managed Services

Las Vegas Service Center (RH)
- Secure Data Hosting
- Virtual Workspaces
- Managed Document Review
- E-Discovery
- Contract Review and Remediation
- Records/Legal Holds Management

Legal Consulting Global Ops Center (RH)
## CYBERSECURITY AND PRIVACY: WHAT’S TRENDING IN THE MARKETPLACE

<table>
<thead>
<tr>
<th>Practice</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organizations are Creating a Digital Trust and Safety Team to Maintain the Integrity of Interactions Wherever the Consumer Meets the Brand.</strong></td>
<td>There is a growing trend in B2C organizations that providing an environment where their customers feel safe and secure is a business differentiator.</td>
</tr>
<tr>
<td><strong>Manage the Cost of Cybersecurity.</strong> Respondents to CIO.com’s 2020 State of the CIO study are definitely concerned: a full 34% saw security and risk management as the number one driver of IT spending overall at their organization.</td>
<td></td>
</tr>
<tr>
<td><strong>AI Creates New Security Responsibilities for Protecting Digital Business Initiatives and Security Tools that use AI and Defending Against AI-Based Attacks.</strong></td>
<td>AI will evolve from being predominantly perceived as a marketing term to a critical technology for improved threat detection.</td>
</tr>
<tr>
<td><strong>Build Your Organization’s Cyber Resilience.</strong> According to Gartner, by 2025, 70% of CEOs will mandate a culture of organizational resilience to survive coinciding threats from COVID-19, cybercrime, severe weather events, civil unrest and political instabilities.</td>
<td></td>
</tr>
<tr>
<td><strong>Security Process Automation is Emerging to Eliminate Repetitive Tasks.</strong> Security buyers should elevate the automatability of administrative tasks in new purchases and seek solutions that have robust and well-documented APIs, and a healthy partner ecosystem with prebuilt integrations for automation.</td>
<td></td>
</tr>
<tr>
<td><strong>Zero Trust Network Access Technology Is Beginning to Replace VPNs.</strong> While ZTNA offers clear security advantages over the traditional VPN approach, in most enterprises, full-scale adoption of ZTNA will be slowed because they do not have an accurate mapping of which users need access to which applications.</td>
<td></td>
</tr>
<tr>
<td><strong>Address the Talent Gap.</strong> 62% of CISOs think the global cybersecurity talent shortage will get worse over the next five years, according to Global Snapshot: The CISO in 2020. Security leaders should explore unconventional ways to attract passionate learners.</td>
<td></td>
</tr>
<tr>
<td><strong>A Full Lifecycle Approach is Emerging for Protection of the Dynamic Requirements of Cloud-Native Applications.</strong> The unique and dynamic requirements for protecting cloud-native applications will require a lifecycle approach for protection spanning development and production. This approach will use offerings designed for protecting cloud-native environments.</td>
<td></td>
</tr>
</tbody>
</table>

Sources: Gartner, CIO.com, Security Magazine

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
# Cybersecurity and Privacy: Understanding Your Perspective

## The Challenges Clients Bring

- Automate, mature and manage new digital security challenges while protecting data and business assets
- Privacy pressures from increased regulation (GDPR, CCPA, etc.) and scope of compliance
- Resource shortages and skills for cybersecurity and privacy needs
- Securing the journey to the cloud and new technologies
- Respond, recover and build resilience in the face of an adverse event (e.g., data breach)

## The Answers Clients Are Looking For

- Design, implementation and management of new cyber capabilities and technologies across domains of Identify, Protect, Detect, Respond and Recover
- Implementation of regulatory compliance, privacy and third-party risk management programs, while establishing trust with stakeholders
- Deep subject matter expertise with a flexible delivery model, including bringing in the right partners
- Efficient and effective transition to, compliance with and management of the cloud, while leveraging new technologies (e.g., AIML)
- Design and implementation of resilience solutions and processes to withstand disruptive events

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
Securing your future with trust and confidence.

As technology rapidly evolves and digital adoption accelerates, Protiviti’s cybersecurity and privacy team turns risk into an advantage – protecting every layer of an organization to unlock new opportunities, securely.
HOW WE CAN HELP YOU

MANAGE YOUR SECURITY STRATEGY AND ENABLE COMPLIANCE AND TRUST
- Cybersecurity Operating Model Enablement
- Cybersecurity and Privacy Risk Assessments
- Reporting Transparency and Compliance
- Digital Security Governance Optimization

PROTECT YOUR DATA AND BUSINESS ASSETS
- Data Security Strategy and Readiness
- Technology Risk and Vulnerability Management
- Access Management
- Data and Privacy Management

TRANSFORM AND OPTIMIZE YOUR BUSINESS
- Process Design and Execution
- Software Security Acceleration
- Security Tools Optimization and Rationalization
- Customer Experience Optimization

ARCHITECT YOUR SECURITY PLATFORMS
- Zero Trust Architecture
- Intelligently Automated Security
- Secure and Flexible Architecture Engineering
- Cybersecurity Systems Design and Implementation

SUSTAIN YOUR SECURITY PLATFORMS
- Security Operations Management
- Risk and Continuous Control Monitoring Management
- Workforce Effectiveness Enablement
- Resource Competency and Capacity Management

ENABLE YOUR SECURITY RESILIENCE PLANS
- Fraud and Crisis Fusion Center
- Third Party Risk Management
- Business Continuity and Transparency
- Resilience Assurance

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
Protiviti’s Cybersecurity and Privacy team combines deep technical security competence with executive-level communication and management. Our holistic approach starts by understanding what is most important to organizations, then structuring and supporting programs so your business is engineered to grow securely.

**Security Program and Strategy**
- Risk Assessment and Analysis
- Program Design, Benchmarking and Metrics
- Policy Design and Development
- Security Strategy and Governance
- Board/C-Suite Cybersecurity Communication and Reporting
- Cyber Program Office

**Cloud Security**
- Strategy, Architecture and Implementation
- Cloud Security Assessment
- DevSecOps
- Cloud Vulnerability Management

**Data Security**
- Data Classification, Protection and Governance
- Compliance (e.g., PCI, HITRUST, FFIEC)
- Cyber Defense
- Vendor/Third-Party Risk Management

**Attack and Penetration**
- Application Security Testing
- Network Security Testing
- Red Team
- Social Engineering
- DevSecOp SDLC
- Source Code Review
- Hardware, IoT and Medical Device Testing
- Vulnerability Management

**Managed Security Services and Security Ops**
- Managed Detect and Respond (MDR)
- Threat Vulnerability Management
- Managed Cloud Security Ops

**Digital Identity**
- IAM Program and Strategy
- Role-Based Access Control
- Identity Governance and Administration
- Privileged Access Management
- Access Management
- Directory Services

**Incident Response and Cyber Resilience**
- Strategy and Planning
- Tabletop Exercises
- Emergency Breach Response
- Cyber Forensics and Litigation Support
- Compromise Assessments
- Cyber Threat Hunting
- Business Continuity/Business Resiliency
- Post-Event Review/Facilitated Lessons Learned

**Operational Resilience**
- Enterprise Resilience Programs
- Formalizing Business Services
- Cyber Resilience
- Technology Resilience
- Business Resilience
- Third-Party Resilience
- Resilience Testing and Assurance

**Data Privacy**
- Privacy Program Assessments
- Privacy Program Development
- Privacy as a Service (PraaS)
SECURITY PROGRAM AND STRATEGY

CLIENT PROBLEMS WE SOLVE

Gaining clarity on ever-increasing information security-related risks and their impact to the organization; quantifying and defining the risk tolerance and developing/refining strategies and controls to address those risks.

The challenge to build and operate an infrastructure that preserves the integrity and confidentiality of the organization’s data assets and intellectual property.

Communication effectiveness to a variety of stakeholders, from operational management to C-suite leadership and boards of directors.

Insufficient skills or operational resources to manage and deliver security program initiatives.

BUSINESS OUTCOME

ENVISION
Understand information security threats and current capabilities to deal with them, and design necessary improvements

REALIZE
Set a strategic course and implement the designed architecture, leveraging strong program/project management and quantifying risk to articulate the benefit of doing so

PROTECT
Meaningful communication of progress and results to stakeholders that matter most – the board, employees, partners and customers – and driving continuous improvement

OUR STEPS TO SUCCESS:

- Drive clarity on information security and privacy strategies; quantify and align them with business objectives
- Establish the cybersecurity program office’s foundation and strategy; manage work streams and improve security programs
- Implement security program design, benchmarking, strategy, architecture, policies, metrics and awareness of program objectives
- Ensure board/ C-suite cybersecurity communication and reporting, training and awareness
SECURITY PROGRAM AND STRATEGY

Client Challenge
A global life insurance company sought assistance in building a cloud platform with appropriate controls to provide high-availability (HA) applications for their clients. Specifically, the client wanted to develop a target control structure and framework for a cloud platform.

Solution Delivered
Evaluated maturity of the risk management organization, including target capabilities and new areas of focus
Analyzed existing Agile delivery and continuous integration models; defined and implemented key security controls for a DevSecOps pipeline
Identified opportunities for organizational and procedural change supporting cloud integrations
Developed prioritized security reference architecture patterns to establish repeatable guidelines for cloud initiatives

BUSINESS RESULTS
- Provided assessment of existing capabilities and new requirements necessary for cloud transformation
- Created roadmap for DevSecOps integration with existing Agile environment
- Provided expertise on existing process changes required to support cloud integrations
- Created sustainable cloud security architecture for repeatable processes

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
Our national and global clients are experiencing an unprecedented change in the data privacy landscape. Numerous new and changing U.S. state and federal regulations, as well as global regulations, are forcing business, technical and legal operational changes on a nearly weekly basis. These changes are not necessarily exclusive of one another and often overlap, resulting in highly complex legal and regulatory scenarios.

Protiviti supports our clients by helping them establish effective privacy compliance programs that cross the legal, technical, business and compliance groups. Our approach ensures that clients' privacy programs meet or exceed their legal data privacy obligations in an efficient and cost-effective manner.

<table>
<thead>
<tr>
<th>OUR STEPS TO SUCCESS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish a formal inventory of data processing operations and supporting systems that collect, process and store personal data</td>
</tr>
<tr>
<td>Perform a current-state analysis against the requirements to identify gaps and develop a roadmap to achieve compliance</td>
</tr>
<tr>
<td>Implement appropriate solutions to remediate gaps and achieve compliance. Establish all components of data privacy compliance program</td>
</tr>
<tr>
<td>Conduct ongoing monitoring of compliance data, privacy protection and changes to legal obligations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BUSINESS OUTCOME</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENVISION</td>
</tr>
<tr>
<td>Understanding data collection, processing and applications in scope; identification of regulatory compliance gaps and remediation steps to quickly achieve compliance</td>
</tr>
<tr>
<td>REALIZE</td>
</tr>
<tr>
<td>Implementation of an effective and flexible data privacy program that meets not only today's obligations, but those of tomorrow as well</td>
</tr>
<tr>
<td>MANAGE</td>
</tr>
<tr>
<td>Support client data privacy obligations by providing a managed services/outsourced option to the GC and CIO groups</td>
</tr>
</tbody>
</table>
### Client Challenge

A global insurance company with operations, customers and employees in 23 countries needed to create an effective data privacy program that addressed not only U.S. data privacy regulations, but global regulations as well. Trying to meet the individual regulations using a "one-off" approach was not only legally risky, but also inordinately expensive.

The nature of data processed globally by the organization, along with the complex, overlapping legal jurisdictions (e.g. CCPA, FCRA, GDPR, etc.) that they fell within, required a common, comprehensive and flexible data privacy compliance approach. In addition, the company needed global training and communications, governance and strategic support.

### Solution Delivered

- Developed an executive report summarizing the organization's privacy requirements and potential risks, educating leadership on an effective path to compliance
- Produced a detailed analysis addressing key privacy compliance gaps and root causes, along with a remediation plan
- Implemented a common and flexible data privacy compliance program globally
- Introduced a vendor-contract review program, including a standardized assessment template and DPIA template framework and approach
- Created a managed services model to support customer requests

### BUSINESS RESULTS

| Issued detailed and executive data privacy regulatory assessment reports | Increased enterprise data privacy awareness across the organization using state-of-the-art organizational change management techniques | Implemented effective and flexible data privacy compliance program globally | Established a managed services/outsourcing model that moved data subject requests processing to Protiviti |
## DATA SECURITY

### CLIENT PROBLEMS WE SOLVE

Design, implement, operationalize and validate data security technology and programs supporting PCI, HIPAA, GLBA and FTC compliance requirements.

Implement data governance and protection.

Design and implement security architecture, including physical and cloud firewalls, security engineering and zero-trust network design.

### BUSINESS OUTCOME

#### ENVISION

Understanding of data collection, processing and applications in scope; identification of compliance gaps and remediation steps to achieve compliance

#### REALIZE

Implementation of improvements and solutions to protect data

#### PROTECT

Data protection controls embedded throughout the organization

### OUR STEPS TO SUCCESS:

- Determine security goals and objectives and translate them to technical requirements
- Determine gaps between current processes, tools, architecture and desired outcome
- Architect a technical solution including sourcing third-party products
- Implement and test the technical solution
## DATA SECURITY

### Client Challenge

A global technology company was unable to address the totality of their security compliance requirements. The company lacked both the knowledge and the headcount necessary to address its customers’ vast and disparate compliance requirements, which included FedRAMP, PCI, SOC 1 & 2, HITRUST, ISO 27001, alignment with FFIEC and several others. This, combined with strong growth projections for the organization, required the company to expand its current team and also consider how to respond to future compliance maintenance necessities without constantly having to add headcount.

### Solution Delivered

- Fielded a team of Protiviti professionals qualified to support the required security standards
- Facilitated interactions between the client process and control owners and third-party certification/attestation bodies
- Developed standardized reporting and communication protocols for tracking compliance status, ensuring leadership is made aware of progress and potential roadblocks
- Analyzed repeatable compliance processes that could be standardized and offshored

## BUSINESS RESULTS

<table>
<thead>
<tr>
<th>Key security compliance deadlines were met</th>
<th>Increased support for control and process owners, allowing them to focus on their own operational goals and objectives</th>
<th>Client’s customers were able to place more reliance on organization’s control environment</th>
</tr>
</thead>
</table>

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
The proliferation of services and features available on cloud platforms, coupled with underinvestment in training on how to protect specific use cases, leads to unmanaged complexity.

Lack of visibility into the type of information being processed in the cloud and which users have control to manipulate data, services and infrastructure results in poorly governed cloud footprints.

Organizations are not taking advantage of the efficiency and effectiveness opportunities that exist through automation and orchestration, and the outcome is manual, people-dependent processes that do not scale.

**OUR STEPS TO SUCCESS:**

- Determine security goals and objectives and translate them to technical requirements
- Determine gaps between current processes, tools, architecture and desired outcome
- Architect a technical solution including sourcing third-party products
- Implement and test the technical solution

**BUSINESS OUTCOME**

**ENVISION**

Improved confidentiality, effective controls over information access, and compliance with legal and regulatory mandates

**REALIZE**

Reduced risk of data and system compromise; greater confidence in security effectiveness due to automation and coverage of security controls

**PROTECT**

Business-critical information assets are operating in a secure environment
CLOUD SECURITY

Client Challenge
A global consumer goods conglomerate was advancing the execution of its digitization strategy (which included defaulting to SaaS, PaaS and IaaS options for new IT projects). However, this organization had not designed or implemented protection, secure provisioning and governance frameworks to align with the speed of deployment and to guard against business disruption. As a result, the organization was seeking a partner to develop control governance framework and a technical cloud security reference architecture to support their "cloud first" digital strategy.

Solution Delivered
Developed foundational cloud security controls for SaaS, PaaS and IaaS cloud computing categories

Designed identity, information protection and operations security reference architectures to meet security requirements and incorporate budgetary and risk-based decision criteria

Analyzed and documented use of "sanctioned" versus "unsanctioned" applications to ensure compliance with internal and regulatory requirements

Developed standardized reference architectures to provide stakeholders with security principles that can drive self-service assessments

BUSINESS RESULTS

Accelerated decision making for product teams and stakeholders, thus eliminating the cybersecurity team as a bottleneck for innovation

Created detailed roadmap to support ongoing journey to maturity of the cloud security program and reduce probability of noncompliance with HIPAA, PCI and GDPR

Documented security capabilities for SaaS, IaaS and PaaS platforms to enable benefits of modern technologies without diminishing security of customer information

Developed common language for executives and business stakeholder to discuss governance of their digital transformation initiatives

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
**DIGITAL IDENTITY**

**CLIENT PROBLEMS WE SOLVE**

- Effective management or reporting of user access, access privileges, audit trails, and when or how privileged accounts are being used, including by third-parties hosting client servers or applications.
- Remediation of audit or regulatory requirements for controlled access or least privileged.
- Changes in security management due to mergers, acquisitions or divestiture of business entities

**BUSINESS OUTCOME**

**ENVISION**

Assess and baseline current environment to identify gaps; develop IAM program strategy with a centralized onboarding approach and control framework

**REALIZE**

Reduced risk of data breach with an improved security posture, including efficiencies on the organization's access lifecycle; reduced reliance on manual controls

**PROTECT**

Establish single view of user's access catalog; implement automated solutions to manage access

**OUR STEPS TO SUCCESS:**

- Define IAM strategy and roadmap
- Develop IAM operating model
- Implement IAM and PAM solutions; remediate compliance issues
- Establish governance model to support business objectives
This global specialty hospital corporation had recently been spun off from its parent and had two years to implement its own IAM program, systems and processes. Although the client had its own subdomain, many of its systems and users were joined to the parent’s corporate domain; identity governance technologies and IAM processes were owned and operated by the parent company.

Selected and implemented IAM solution for provisioning for Active Directory and 110 business applications and systems
Supported the migration of Active Directory domains
Implemented IAM governance model and reporting to monitor access

Timely migration to new domain and implementation of provisioning solution
Creation and implementation of "run books" to migration of users, computers and applications to the new domain
Automated provisioning for distribution lists and shared drives
### ATTACK AND PENETRATION

<table>
<thead>
<tr>
<th>CLIENT PROBLEMS WE SOLVE</th>
<th>BUSINESS OUTCOME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help organizations gain an understanding of their specific threat landscape, including security vulnerabilities, root causes and remediation options.</td>
<td><strong>ENVISION</strong></td>
</tr>
<tr>
<td>Protect sensitive data and systems to avoid costly breaches, loss of intellectual property, business disruption and reputation damage.</td>
<td>Understanding of security vulnerabilities and specific threat landscape, including how potential issues may impact businesses</td>
</tr>
<tr>
<td><strong>REALIZE</strong></td>
<td></td>
</tr>
<tr>
<td>Remediation of security vulnerabilities and threats in the environment</td>
<td><strong>PROTECT</strong></td>
</tr>
<tr>
<td>Reduced risk of data breaches</td>
<td></td>
</tr>
</tbody>
</table>

### OUR STEPS TO SUCCESS:

- Periodic internal and external vulnerability assessments or manual penetration tests of the environment
- Consistent, on-demand security testing across networks, applications, IoT, hardware and more
- A managed, risk-based testing program with remediation oversight to maximize ROI
## Client Challenge

A global supermarket chain was undergoing a significant technology change which required a number of investments and updates to applications, systems and networks. The Security team was tasked with deploying a method to ensure that the new technologies were being implemented in a secure manner that prevented unauthorized access. However, the team was not able to quickly source or train the talent needed to perform these technical reviews on such a wide array of technologies. The client needed an "on-demand" solution that would allow it to quickly spin up testing and meet dynamic business deadlines.

## Solution Delivered

Developed penetration testing-as-a-service solutions that allowed the client to respond to changing needs

Deployed red and purple teams to aggressively challenge plans, policies, systems and assumptions while verifying the technologies' capabilities

Developed network-level testing and static web application assessments

Implemented wireless reviews for various stakeholders within the client organization

## BUSINESS RESULTS

| A defined process for business and IT leaders to assess new technologies before implementation to better understand risk and impact of potential vulnerabilities. | Significant reduction in the organization's overall security risk through the identification of hundreds of critical network, system and application vulnerabilities which might have allowed attackers access to sensitive systems and data if left undiscovered or unfixed. | A more thorough understanding of potential business impact (data loss, significant system downtime, etc.) for known/accepted issues in the environment. | In many cases, confirmation that technologies have been designed, configured and deployed in a secure manner. |

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
# MANAGED SECURITY SERVICES AND SECOPS

## CLIENT PROBLEMS WE SOLVE

Keeping pace with changing business demands.

Limited market availability of qualified resources; staff retention challenges.

Rapid responses necessary to satisfy critical functions, including critical security incidents and IT risk management and controls.

Immediate demand for solutions to secure and protect assets and data.

## BUSINESS OUTCOME

### ENVISION
Scalable, contractual teams and services in simple solution frameworks with skilled resources

### REALIZE
Optimize the delivery of repeatable processes, emerging compliance changes and transformative business process changes

### PROTECT
Optimize compliance activities by successfully achieving business strategies and objectives

## OUR STEPS TO SUCCESS:

- **Scan digital technology infrastructures for existing vulnerabilities and remediate cyber threats**
- **Build a unified security program that increases visibility, automates threat detection and response, and delivers actionable metrics for continued improvement**
- **Monitor cloud resources to continuously assess and measure data, applications and infrastructure behaviors for potential security threats**
## Client Challenge

Improving overall enterprise resiliency and providing additional capabilities for the client's current security operations center (SOC) to accelerate identification and remediation of its critical Tier 3 security events.

Engagement is technically complex within the customer outsourcing network infrastructure, with two outsourced network service providers providing critical services.

## Solution Delivered

- Developed incident identification and incident response playbooks
- Implemented tools in third-party SIEM platform
- Developed procedures for Tier 3 event ID and response
- Managed response execution by setting up a scalable onshore/offshore response capability
- Performed threat hunting within the internal network

## BUSINESS RESULTS

- Provided a unique Managed Detection and Response (MDR) offering, leveraging onshore and offshore capabilities
- Adjusted delivery model and team composition as MDR services scaled up
- Embedded scaling factors based on number and complexity of client MDR requirements
- Expanded vendor partnership

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
## INCIDENT RESPONSE AND CYBER RESILIENCE

### CLIENT PROBLEMS WE SOLVE

- Uncertain organizational response to handling security incidents and related outages.
- Unseen threat actors may have bypassed traditional defenses and detection.
- Complex security incidents requiring specialized skills, tools and knowledge.
- Rigid incident response programs are unable to counter dynamic threats.
- Lack of business continuity and/or resiliency strategies, documentation and response plans.

### BUSINESS OUTCOME

#### ENVISION
Discover and respond to otherwise unseen cyber attacks and related outages

#### REALIZE
Effective strategies for detecting and responding to threat actors; coordinating the entire organization's reaction to security incidents, from initial discovery through reporting to the board; ensuring continuity and resiliency plans are well designed, documented and tested

#### PROTECT
Enhance confidence in the business by offering strategic planning, meaningful practice, detection of unseen attacks through compromise assessments, and comprehensive response to actualized threats, while ensuring continuity and resiliency plans are in place to protect the enterprise

### OUR STEPS TO SUCCESS:

<table>
<thead>
<tr>
<th>Incident response strategy and planning; business continuity and resiliency planning</th>
<th>Compromise assessment; tabletop and breach response; cyber threat hunting</th>
<th>Forensic discovery and analysis; post-event review and facilitated lessons learned</th>
<th>Documented and tested business continuity and resiliency plans</th>
</tr>
</thead>
</table>

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
## INCIDENT RESPONSE AND CYBER RESILIENCE

### Client Challenge

A global e-commerce provider was approached by acquiring banks about common point-of-purchase correlations, indicating that the provider may be compromised. The client needed to:

- Identify PCI gaps and deliver remediation as a demonstrable act of diligence
- Develop and implement a global strategy to identify the alleged breach
- Gather information for external counsel to use in formulating a regulatory response
- Preserve evidence under the direction of counsel for anticipated litigation
- Develop strategic guidance in conjunction with counsel during an independent PFI investigation

### Solution Delivered

Provided on-site team in forensic/incident response and PFI investigations to build a response strategy

Gathered global evidence preservation and tracking for regulatory, PCI and potential litigation strategies

Delivered a security remediation program to establish diligence in response

Provided articulation and support for key elements of external counsel's strategy for answering requests from privacy regulators

Provided interpretation and articulation of cyber threat intelligence used to identify the true source of the CPP data, establishing that client systems were not breached

### BUSINESS RESULTS

| Privacy regulators accepted the assertion that global systems were not the source of data exposure | Avoided millions of dollars in potential PCI fines by making timely and accurate disclosures | Presented an accurate narrative of events that was legally defensible, and defused negative publicity | External counsel received demonstrably accurate answers to questions during the formation of strategy |

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
## OPERATIONAL RESILIENCE

### CLIENT PROBLEMS WE SOLVE

The ability to detect, respond to, manage and recover from a disruptive event, whether initiated from cyber, natural disasters, technology or human error.

Aligning with new and evolving regulations with regard to operational resilience.

Taking advantage of opportunities to increase resilience of business services through trusted approaches and innovative solutions.

Integrated testing efforts, which allows firms to demonstrate their ability to recover from events and improve upon weaknesses in current processes and services.

### BUSINESS OUTCOME

#### ENVISION

Assess current practices around operational resilience, including assessment of foundational elements.

#### REALIZE

Analyze existing business services to determine criticality, establish initial impact tolerance methodology and create economic impact scenarios.

Design and implement a resilience program with a focus on governance and alignment.

Address cyber resilience and third-party deficiencies.

#### PROTECT

Conduct testing to simulate "extreme but plausible" scenarios impacting critical business services; in partnership with executive leadership, integrate resilience standards into all standard business and IT audits and foundational audits (e.g., cybersecurity, third-party).

### OUR STEPS TO SUCCESS:

- **Establish a clear understanding of critical business services, including a clear front-to-back mapping of processes, third-parties and systems that support the service.**
- **Take advantage of and adapt to existing programs and initiatives to better integrate resilience into the environment.**
- **Build resilience by designing and implementing essential programs to withstand adverse changes.**
- **Orchestrate across the enterprise on operational resilience. Break down silos that exist across business and technology functions.**
## OPERATIONAL RESILIENCE

### Client Challenge

This global and systemically important financial institution had been given a regulatory mandate to address the operational resilience of their organization. This mandate, driven by the first line, included assessing planned initiatives against leading practices and enhancing plans where necessary; helping to draft regulatory responses; developing a go-forward strategy for the first line, including criticality framework, resilience operating model and testing approach; and working with the second line to develop appropriate metrics to monitor resilience and challenge first-line efforts.

### Solution Delivered

- Performed a current state assessment of operational resilience efforts, benchmarking against regulatory expectations and leading practices
- Created a go-forward plan that accounted for work efforts to date and organizational/system limitations to address resilience concerns
- Embedded Protiviti consultants and subject matter experts across the delivery workstreams, aligning the client’s efforts with operational resilience leading practices and regulatory expectations from a global set of regulators
- Aligned regulatory response with pragmatic go-forward efforts, ensuring plans exceeded regulatory demands

### BUSINESS RESULTS

| Created a global resilience strategy and operating model to align the organization with pending regulator demands | Provided guiding principles, frameworks and industry/regulatory insights to allow for advancement of resilience efforts and enhanced board/management reporting | Created a framework to address and validate the organization’s critical business services | Developed a customized strategy and approach for resilience capability testing |
Face the Future with Confidence