SERVICES

PLANNING *(SECURE TECHNOLOGY SOLUTIONS)*

Technology vendors (such as those selling and supporting hardware, software, SaaS solutions and other services) can't be expected to be cybersecurity experts simply by being experts in their solutions. It takes thorough planning effort to ensure any technological solution being deployed will meet all the defined security and compliance requirements while remaining cost-effective. Whether one is dealing with an ERP system, updates to the financial management software, or a deployment of a new e-commerce website, proper planning is necessary for a consistent and secure treatment of data and can ensure maintenance of organizational regulatory and legislative compliance by taking security into account from the very start. Good planning – occurring certainly before deployment, if not before vendor selection – is paramount to ensuring successful project delivery and meeting corporate objectives, saving an organization from having to rework or even replace its recent IT investment due to discovery of material weaknesses in the solution design that would have otherwise been foreseeable. Whether a company intends to deploy new technology, put in compensating controls to reduce the risk associated with an old critical system, or simply wants to streamline its operations through automation or outsourcing, integrating secure technology planning activities into all future IT projects is always in its best interest.

CATEGORIES OF SERVICE OFFERINGS

1. Security Architecture and Design

Considerable risk and investment require significant planning to support execution of a successful project. Beyond vendor claims of their turn-key deployments that will solve all known and unknown customer problems, only a thorough planning process can identify all the requirements specific to an organization and narrow down the solutions that limit costs while enabling the business to succeed. Establishing risk parameters as part of project planning and evaluating designs in terms of that risk is imperative to securing the deployment of critical enterprise systems – understanding which controls are needed and where they should be placed to mitigate risk effectively is similarly paramount to minimizing both the implementation and maintenance costs.

Our Security Architecture and Design services include:

- *Business Driven Security Architecture*
    - Align architecture with strategies
    - Navigate approval process
    - Develop deployment-ready solutions

- Develop detailed documentation
  - ✓ Functional requirements documents
  - ✓ Non-functional requirements documents
  - ✓ Formalize zones of trust and control
  - ✓ Conceptual architecture diagrams and documents
  - ✓ Logical architecture diagrams and documents
  - ✓ Physical architecture diagrams and documents
  - ✓ Architectural decisions document
- Ensure architecture is consistent with frameworks like:
  - ✓ SABSA
  - ✓ TOGAF
  - ✓ Zachman

- *Regulatory Scope Limitation Design*
  - Provide a data-centric approach to design
  - Integrate with business-driven security architecture approach
  - Consider relevant guidelines when regulated data is used
    - ✓ Financial: Sarbanes-Oxley, CSOX, etc.
    - ✓ Credit Card Data: PCI DSS
    - ✓ Non-public Personally Identifiable Information: PIPEDA, PIPA, FOIPPA, GDPR, CCPA, etc.
  - Limit and define the minimum scope subject to regulation
    - ✓ Consider integrated devices and systems
    - ✓ Consider adjacent devices and systems
    - ✓ Consider devices and systems used to manage and administer
  - Select appropriate technology for scope reduction
    - ✓ i.e. for Ecommerce choose API vs. redirect vs. iFrame
  - Ensure strong boundary controls between different security zones
    - ✓ i.e. firewalls, routers, virtualization, encryption, etc.
  - Provide evidence of a clear understanding of data flows
    - ✓ Conceptual data flow diagrams
    - ✓ Logical and physical data flow diagrams

2. Legacy System Data Security Solutions

It is often difficult to secure older technology whose use is still needed, and replacement of it can be non-trivial either because a company has already invested significantly into it, both financially and through complicated integrations, or because there are no adequate replacements that provide same or similar functionality, and another custom-built system would inevitably and quickly result in comparable vulnerabilities. Environments using mainframe, midrange systems, operational technology, or even instances where the developer of a critical custom software no longer supports it, all qualify as legacy systems that need different types of support than newer technology. Older software and systems are more inclined to have significant security issues but

fixing those becomes far more problematic as the hardware and software continue to age, necessitating replacement as the only feasible long-term solution. Capital planning processes for that inevitable replacement can sometimes take years, but that doesn't mean organizations cannot do something to reduce the risk those legacy systems pose while operating until their decommissioning. With Privity's help, companies can develop and execute risk management strategies to reduce security issues legacy systems bring to their environments, bridging the gap between yesterday's technology and the future.

Our Legacy System Data Security Solutions services include:

- *Isolating systems through technology*
  - Segment legacy system with network technology
  - Limit risk exposure of legacy systems to the rest of the enterprise
- *Modernization of technology*
  - Virtualize legacy systems
    - ✓ Create VMs of end-of-life or out-of-support operating systems
  - Transition some services from legacy equipment
    - ✓ i.e. moving authentication from OS360/OS400 to Active Directory
  - Reengineer and transform business processes
    - ✓ Retire legacy system
    - ✓ Replace with a cloud solution
- *Devaluing data, tokenization, expiration*
  - Evaluate data to determine what can be purged
    - ✓ Identify data that has expired
    - ✓ Identify data that is unnecessary for business purposes
  - Abstract data from the legacy system through tokenization
    - ✓ Store valued data with third-party tokenization service
    - ✓ Design internal tokenization solution reliant on modern technology that can be secured and reduce the risk on the legacy equipment
  - Use masking or hashing to devalue data
    - ✓ Permanently alter the data
    - ✓ Remove critical portions of the data
    - ✓ Make data unusable to third parties who may obtain it through unintended channels

3. Modernization and Transformation

COVID-19 has been said to have triggered more than a decade's worth of IT modernization and transformation occurring in less than a year – but that acceleration only ensured most of the security planning didn't occur, and the related precautions were not taken due to too fast of a deployment. Modernization initiatives – be it moving to a fully-remote workforce or transforming

one's organization by implementing comprehensive operational automation – requires a thorough understanding of the requirements associated with securing the information assets and systems before implementing any technological changes. Without this understanding, appropriate security controls cannot be determined, likely resulting in data being exposed to new unwelcome threats.

Our Secure Modernization and Transformation services include:

- *Transition to cloud services from on-premises or traditional IT*
    - Facilitate migration to Microsoft 365
        - ✓ Design secure collaboration solutions using tools like Exchange, SharePoint, Teams, Kaizala, Yammer, Stream, Viva, etc.
    - Leverage remote or employee-owned computers and mobile devices
        - ✓ Design endpoints security solutions with tools like System Center Configuration Manager, Intune, etc.
    - Reduce software support and licensing fees with a transition to web versions of desktop applications (like Word, Excel, PowerPoint, etc.)
    - Protect corporate data using data loss prevention technology
        - ✓ Prepare for implementation of Microsoft Information Protection
    - Lift and Shift to Cloud (Azure / AWS)
        - ✓ Prepare to move physical servers or locally hosted virtual machines to the cloud
- *Transforming the enterprise to modern processes*
    - Refactor legacy, traditional, or other on-premises applications to Cloud-native
        - ✓ Design solutions using containers, serverless, IaC, etc.
        - ✓ Design solutions that leverage automation and orchestration with autoscaling
        - ✓ Consider emerging technology like IoT and blockchain
    - Implement DevOps / DevSecOps / DevNetOps / etc.
        - ✓ Prepare for Azure DevOps implementation
        - ✓ Design business processes for secure implementation

4. Planning for Secure Outsourcing

Whether planning to outsource some or all of their IT functions to a Managed Services Provider (MSP), Managed Security Services Provider (MSSP), Cloud Service Provider (CSP), or any other third party who will have responsibility for securing the critical data and its processing, companies must understand the value of the said data, the risk that provider poses, and the controls needed for the companies to protect themselves from all the outsourcing downsides. Engaging the right outsourcer requires planning and careful consideration of both solutions and related obligations, and the due diligence process cannot be done once the agreements have been signed and the data has been entrusted to the vendor – a new collection of procedures will need to be established to ensure expectations can be met during the entire lifecycle of the outsourcing relationship.

Our Planning for Secure Outsourcing services include:

- *RFP/RFI Content Development and Solution Selection*
  - Develop requirements for RFPs and RFIs
    - ✓ Business-driven requirements development
    - ✓ Confidentiality of data
    - ✓ The integrity of processing and data
    - ✓ Availability of data and systems
    - ✓ Compliance obligations and expectations
  - Capture requirements in RFPs and RFIs
    - ✓ Establish mandatory data security and compliance requirements
    - ✓ Establish optional or "nice to have' criteria
  - Develop scoring methods for evaluating proposals and solutions
    - ✓ Provide tangible cardinal scoring methods
- *Due Diligence Prior to Contracting*
  - Review detailed vendor solutions
    - ✓ Scope validation
    - ✓ Data flow diagrams
    - ✓ Security architecture reviews
  - Review 3rd party audit results
    - ✓ Scope verification
    - ✓ Analysis of PCI DSS / SSAE 18 SOC2 / ISO 27001 / etc.
  - Review vendor policies and alignment confirmation
  - Review BCP/DRP plans
  - Review down-stream service providers
  - Review incident response plan
  - Review penetration tests/vulnerability scans
- *Responsibility Matrix Reviews or Development*
  - Review or develop appropriate data security responsibility assignment and acceptance
  - Formalize compliance obligations
    - ✓ Mapped to regulation, like PCI DSS
  - Outline expectations for incident handling procedures
  - Outline and formalize clear delineation of responsibilities
- *Contract Reviews*
  - Ensure a reference to responsibility matrix exists
  - Ensure performance monitoring metrics are formalized
    - ✓ Service Level Agreement
    - ✓ Security Level Objectives
    - ✓ Billing reviews
  - Ensure appropriate data security responsibilities are formalized
  - Ensure appropriate compliance obligations are formalized
  - Ensure breach notification activities and expectations are formalized
    - ✓ When vendor must inform

        - ✓ What the process to deal with the breach will be
    - Ensure data ownerships and process for retrieval are referenced
        - ✓ Includes data destruction at the termination of the agreement
    - Ensure recurring review of diligence items and right to audit are included

- *Compliance/ Business Impact Assessments*
    - Establish the impact to the company by outsourcing according to the agreement
        - ✓ Change from managing technology to managing a vendor
    - Determine the changes to compliance obligations and the related management program(s)
        - ✓ Impact of privacy, PCI DSS, SOX compliance obligations