Digital transformation: Begin with cybersecurity in mind

November 2020
Prepare for the unexpected

The benefits of digital transformation—speed, easy data access, rapid data analysis, data visualization and related cost savings—can be completely lost or compromised as a result of a cyberattack. Yet, many government organizations have implemented digital transformation projects using emerging technologies without a strategic or proactive approach to cybersecurity and data privacy. Increasingly, these same organizations are encountering costly cyberattacks in the form of socially engineered spear-phishing attacks, business email compromise (BEC) or spoofing attacks and/or ransomware attacks.

Organizations that do not adequately or proactively begin their digital transformation with cybersecurity in mind can experience cyber fraud and cyber data breaches that result in:

- Cyber related lawsuits for cybersecurity negligence related to lack of data privacy
- Federal and/or state regulatory penalties for cybersecurity / data privacy compliance failures
- Negative impacts to an organization’s reputation due to inadequate information security

Since March 2020, government agencies have experienced a dramatic, unexpected increase in people working from home due to the COVID-19 pandemic. As an example, the number of teleworking Department of Defense (DOD) personnel has increased from 95,000 to more than 1 million, with internet connections to the department-wide virtual private network (VPN) growing from 49,600 to 440,000 per day. This largely unplanned transition from office-based network access to remote / home access has created unique cybersecurity challenges for government agencies. As a result, many organizations are now seeking an improved approach to cybersecurity and data privacy to protect their information.

Digital transformation with cybersecurity at the forefront

According to Cybersecurity Ventures1 and Cisco2, the estimated global damages from cyber fraud and data breaches exceeded $4 trillion in 2019 and IBM Security3 reported the average cost of a cyber data breach now exceeds $8.2 million. To combat this growing trend, government organizations are learning that they must place cybersecurity at the forefront of strategic business planning for all digital projects.

**Ask the right questions**

How do agencies begin digital project or digital transformation with cybersecurity in mind? They start all digital project planning by asking the right cybersecurity related questions upfront. The right questions generate deeper discussion and understanding of the current level of cyber defense, potential cyber threats and known cyber vulnerabilities. This information can then be used by cybersecurity experts to develop and implement a customized, strategic and comprehensive cybersecurity program for each digital transformation program.

**20 key cybersecurity questions to consider**

1. Will this project, the government agency involved and/or selected government contractors require access to any of the following types of data or information?
   - Personally identifiable information (PII) of employees and/or partners protected health information (PHI)
   - Payment card information (PCI)
   - Intellectual property (IP)
   - Controlled unclassified information (CUI)
   - Covered defense information (CDI)
   - Classified information (CI)
   - Company sensitive information (CSI)

2. Who will need access to the project and organization data?

3. How will information access be controlled, both internally and with vendors / subcontractors / the public?

4. Where will the project and organization information reside / be stored and how will it be secured?

5. Who will develop and manage the organization’s information governance plan, information system security plan and data resilience or backup plan?

6. Does the government agency have the right people and resources to effectively lead cybersecurity and data privacy strategic planning and implementation?

7. What project and organization data segmentation or compartmentalization (i.e., zero trust data architecture) is needed to protect the information?

8. Does the project or the organization’s data need to be compliant with one or more of the following specific industry cybersecurity or data privacy regulatory or contractual requirements?
   - National Institute of Standards & Technology [NIST] Special Procedure 800-171
   - ISO 27001: Information system security
   - Payment card industry (PCI) Data Security Standards (DSS)
   - New York Department of Financial Services (NYDFS) cybersecurity
   - Health Insurance Portability and Accountability Act (HIPPA) cybersecurity
   - HITRUST Common Security Framework (CSF)
   - DOD Cybersecurity Maturity Model Certification (CMMC)
   - European Union General Data Protection Regulation (GDPR)

9. What identity, access and data control procedures should be implemented, including: encryption, biometrics and multi-factor authentication (MFA)?

10. What cybersecurity vulnerabilities currently exist within the government agency’s email system, network / information system, software applications and endpoints?

11. Does the government agency currently conduct 24/7/365 data monitoring, cyber intrusion detection and cyber incident response for all information? If not, are these services provided by a highly qualified managed security services provider (MSSP)?

12. Has the government agency developed, documented, implemented and tested effective cybersecurity policies, plans and procedures for project information, including:
   - System security plan (SSP)
   - Security assessment report (SAR)
   - Incident response plan—including SLAs for response time to incidents
   - Business continuity plan—including return to operations (RTO)
   - Disaster recovery plan (DRP)

13. Which cyber threat actors (nation-state cyberattack groups, organized criminal cyberattack groups and/or hacktivists) would be most interested in the project, organization, leadership and supply chain information?

14. What cyber threat vectors would cyberattackers most likely exploit within the organization in order to gain access to valuable information?

15. How susceptible are the government’s employees to potential socially engineered spear-phishing cyberattacks and BEC attacks?

16. Does the organization currently outsource their information technology (IT) services to a managed service provider (MSP) or outsource the cybersecurity to a managed security services provider (MSSP)? Is the government agency leadership satisfied with the outsourced IT or cybersecurity services? Is the MSP or MSSP meeting SLA requirements?

17. When did the government organization most recently conduct a cyberattack simulation or tabletop exercise with the organization’s senior leadership?

18. How is the organization evaluating data integrity? What controls and/or standards are being used to assess data integrity?

19. Does the organization have adequate insider threat protection program?

20. How effective is the organization’s cybersecurity education and training program?
Understand federal government policy and the cybersecurity risk management framework

The May 11, 2017 Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, mandated that all federal government agencies plan, develop and submit formal cybersecurity risk management plans to help mitigate the growing adverse effects upon the classified information, sensitive information and controlled unclassified information in their possession.

Develop and implement a strategic cybersecurity risk management program

So, where do agencies start? How do they know which tools and technology to leverage and which cybersecurity regulations must be met? Successful development and implementation of a holistic cybersecurity risk management program for an organization, whether large or small, requires the following actions and a focus on specific areas of understanding.

Take action

- Begin with a series of diagnostic testing of the organization’s information system including:
  - Email threat assessment
  - Network threat assessment
  - Vulnerability assessment
  - Penetration testing
  - Email spear-phishing campaign (based upon social media analysis)

- Create and communicate a proactive and reactive information security policy, information governance, system security plan, records management processes, information security assessment tools, information security training and information security internal controls throughout the organization and the supply chain

- Hire experience, qualified and certified IT and cybersecurity professionals

- Provide effective information security awareness and training programs for all members of the organization, including simulation training and tabletop exercises for the cybersecurity professionals

- Conduct periodic cybersecurity assessments both internally and via independent consultants

- Develop an incident / breach response process

- Create and implement an information assurance business continuity plan

- Select and implement appropriate and affordable information security tools (hardware and software) and technologies (i.e., machine learning, AI, continuous diagnostics and monitoring, predictive data analytics).

- Decide which cybersecurity services to perform in-house and which services to outsource or purchase:
  - Security design / planning, risk management framework services
  - Risk management assessments
  - Security operations center (SOC) managed services
  - Cyber incident response (IR) services
  - Cyber threat intelligence services
  - Cyber education, training and simulation services

Pursuant to the Cybersecurity EO, each agency is required to utilize the National Institute of Standards and Technology (NIST) cybersecurity Risk Management Framework (RMF). Yet, applying the NIST cybersecurity RMF to each unique federal agency is a challenge, especially due to the scope of knowledge required, the cost of implementation and the speed at which the EO requires risk management plans to be developed, submitted and implemented.

Further, the U.S. federal government and many foreign governments are now requiring that all companies, including predominately commercial companies, develop and implement proactive cybersecurity risk management plans to protect valuable information assets, which may impact national security, economic matters, health care, energy, transportation and other vital industries. Thus, cybersecurity is now an organizational risk management imperative for nearly all government agencies and companies worldwide.

The Cybersecurity EO requires U.S. federal agencies to manage risk across the government, holds agency heads personally responsible for network protection and pushes IT modernizations into overdrive.
**Understand the cybersecurity threat landscape within your organization**

Where is the right place to start to improve cybersecurity for a government agency? Start with a holistic assessment of the people within the organization and their level of cybersecurity awareness and education, information governance processes, systems / hardware and software vulnerability, records management and control procedures for information assurance.

Currently, there are numerous generic and industry-specific cyber risk assessment methodologies and tools, some partially automated and others highly automated. Some risk assessment tools align specifically to ISO or NIST standards while other cyber assessment tools focus on certain areas within an organization such as vulnerability assessments, penetration testing and user training.

**Understand the regulatory landscape**

Our nation's cybersecurity regulatory landscape is complex. Each industry has common risk management frameworks with different compliance requirements.

<table>
<thead>
<tr>
<th>Industry</th>
<th>Cybersecurity Risk Management framework</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial services</td>
<td>• New York Department of Financial services (NYDFS)</td>
<td>• Mandatory</td>
</tr>
<tr>
<td></td>
<td>• Security Exchange Commission (SEC)</td>
<td>• Voluntary</td>
</tr>
<tr>
<td>Health care services</td>
<td>• Health Insurance Portability and Affordability Act (HIPPA)</td>
<td>• Mandatory</td>
</tr>
<tr>
<td></td>
<td>• HITRUST – Common Security Framework (CSF)</td>
<td>• Voluntary</td>
</tr>
<tr>
<td>Federal government</td>
<td>• National Institute of Standards and Technology (NIST)</td>
<td>• Mandatory</td>
</tr>
<tr>
<td></td>
<td>• NIST SP 800-Series</td>
<td></td>
</tr>
<tr>
<td>Government contractors</td>
<td>• NIST 800-37 Risk Management Framework (RMF)</td>
<td>• Varies</td>
</tr>
<tr>
<td></td>
<td>• NIST 800-171 Controlled Unclassified Information (CUI)</td>
<td></td>
</tr>
<tr>
<td>Defense contractors</td>
<td>• DFARS 252-204-7012</td>
<td>• Mandatory</td>
</tr>
<tr>
<td></td>
<td>• NIST 800-171 CUI and Covered Defense Information (CDI)</td>
<td>• Mandatory</td>
</tr>
<tr>
<td></td>
<td>• DOD Cybersecurity Maturity Model Certification (CMMC)</td>
<td></td>
</tr>
<tr>
<td>Accounting services</td>
<td>• American Institute of Certified Public Accountants (AICPA) System for Organizational Controls (SOC)</td>
<td>• Voluntary</td>
</tr>
<tr>
<td>Retail industry</td>
<td>• Payment card industry (PCI)</td>
<td>• Mandatory</td>
</tr>
<tr>
<td></td>
<td>• Qualified Security Accessors (QSAs)</td>
<td></td>
</tr>
<tr>
<td>Multinational companies</td>
<td>• International Standards Organization (ISO)</td>
<td>• Varies</td>
</tr>
<tr>
<td></td>
<td>• ISO 27001</td>
<td></td>
</tr>
<tr>
<td>EU Citizen</td>
<td>• European Union (EU)</td>
<td>• Mandatory</td>
</tr>
<tr>
<td></td>
<td>• General Data Privacy Regulation (GDPR)</td>
<td></td>
</tr>
</tbody>
</table>
Understand how new technologies and tools can cost effectively optimize cybersecurity risk management

New information security technologies, new security tools (hardware and software) and expanded cybersecurity professional services are being developed and implemented nearly every day to stay abreast of the increasing cyber threats and attacks.

Today, most information security practices and controls are focused on protecting vital information assets from future cyberattacks. The new technology trend in information assurance is a fundamental shift in strategy that assumes IT systems have already been breached and then implements:

- Machine learning with mathematical concepts of probability to discover breaches and rapidly respond by developing software remedies
- Artificial intelligence enabling the system to self-diagnose and implement fixes as needed in real time
- Data and threat visualization tools (i.e., Splunk data analytics tools, RSA cybersecurity dashboards)
- Real-time total network immersion technology
- User, mobile devices and network correlation to use predictive analytics to identify abnormal activities, unusual connections and significant changes in volumes of data being moved between machines

Summary

Cybersecurity is not an option, but rather an organizational risk management imperative for all government agencies and companies world-wide. Cyberattacks are on the rise and the potential damages and liabilities are increasing exponentially. Thus, it is vital that all organizations operating in this new digital age assess their information security programs and wisely invest in the necessary resources to protect, detect and recover from imminent cyber data breaches.

Too many organizations, when embarking on large-scale digital transformation for their organization fail to develop a strategic, proactive and threat-based cybersecurity program and consequently under-invest in the following five key elements of cybersecurity.

- Provide appropriate cybersecurity education / training for everyone across the organization using computer-based learning and/or cyber simulations via cyber ranges
- Hire the right people to lead the organization's cybersecurity and data privacy strategic planning and implementation from the start
- Engage independent firms to conduct cybersecurity diagnostic testing, including: computer vulnerability scanning, penetration testing, email system cyberattack assessments, spear-phishing campaigns and dark web analysis, to understand the organization’s cyber vulnerabilities and threats
- Ensure continuous 24/7/365 information monitoring, intrusion detection, and rapid cyber incident response services either internally or via outsourced Managed Security Services Providers (MSSP).
- Implement and test appropriate information resilience plans and procedures via cyber incident response plans, cyber business continuity plans, and disaster recovery plans.

The key to success is to begin all digital transformation projects with cybersecurity in mind. By engaging with cybersecurity experts from the start of a project, or new business venture, a federal, state or local government agency can develop a proactive and threat-based cybersecurity program to achieve information integrity and data privacy through effective cybersecurity.