Beyond Encryption

S. SIngleton

IT system transformations resulting from significant mission or organizational change, dynamically changing supply chain and counterparty networks, even periodic system upgrades can create exploitable vulnerabilities that enable malicious cyber activity.

- Encryption, data masking and traditional de-identification may not be sufficient to provide protection, since observable and "inferable" information is still exposed, particularly during testing with live mission, personnel or agency data.
- Technical and Legal solutions are available to better protect data by disassociating information items such as individuals and organizations from other high-impact information, thereby mitigating reputation, liability and financial exposure.

Security attacks saturate Cyber Space. Breach stories clutter the headlines. Government is pursuing new remedies.

- Legislative and Executive branch leaders are pursuing new tools for better, faster private-public information sharing.
- The technical community – cyber security professionals, IT companies, government agencies like NIST (Framework) and NGOs (SANS Institute, Internet Security Alliance and others) - provide guidance for responsible IT hygiene.

These are necessary steps that may protect against 75% of incidents, yet they are not sufficient, nor do they provide practical ways to protect critical stakeholder interests in cyber-driven national security systems. There is simply too much activity. No one can track, prevent and respond to it all.

While most Federal solicitations do not yet require information protection beyond encryption, the specter of adverse mission, legal and public confidence consequences (major breaches will become public!), argues for consideration of additional measures by acquisition managers and system integrators alike.

If organizations could quantify mission, reputation/geopolitical, financial (budget) and legal/regulatory exposure, they could then develop actionable "risk triage" strategies and take appropriate steps to protect the information whose breach or exploitation present the highest consequence, as well as contain risk management expenditures commensurate with exposure.

- There are in fact sound approaches to quantifying the financial, (geo)political and reputation consequences of cyber risk.
- There are practical information de-identification tools which protect high-impact information from exposure and provide legal advantages.

Cyber Risk From the Complex, Expanding Threat-Space

Critical Infrastructure systems, upon which agencies and institutions rely to conduct the nation's business, are complex adaptive "systems-of-systems," composed of thousands of interdependent components connected through myriad channels. They operate in a rapidly changing socio-political environment that presents threats from individual, group and state actors with shifting alliances, attitudes and agendas. As this eco-system becomes more complex and interconnected, it gives rise to systemic risks and exploitable vulnerabilities that—once triggered—have a runaway effect, with multiple, severe national consequences.

Advanced Persistent Threats (APTs) and accidental or criminal attacks that are often mistaken for APTs, present too many potential crises to manage with limited financial, human and technical resources. They saturate crisis/consequence management resources. Organizations may not recognize the most impactful attacks for minutes, hours, even days.

Most IT product and service providers pursue market strategies that offer new competitive features and short term profits, limiting the amount of time and money invested in security. Reliance upon COTS hardware and software limits the inventory of IT products with certifiably assured performance. The rapid adoption of new technologies, such as social networking, mobility and cloud computing, tips the scales adversely in the trade-off between market demand and security.

Cyber assessments rarely quantify high-impact risks required to prioritize resource allocations. Analyzed against traditional Enterprise Architectures, they cannot measure intricate, dynamic interactions among and between cyber and human elements of mission systems. They cannot isolate exploitable "covert channels," hidden supply chain threats, instabilities, multiple simultaneous faults, or other hidden risks with significant national, economic and public confidence impact. And they do not provide the measures needed to prioritize and triage response strategies commensurate with mission or national interests.

Whereas as much as 75% of the cyber threat can be managed by the IT hygiene and information sharing initiatives promoted by public and industry officials, there is another manageable, yet overlooked cyber risk that cries out for attention.

Mission and organizational transformation programs may present self-inflicted cyber risks

Mission and organizational transformation programs subject critical information assets to exposure from transition and testing activities. Often overlooked, they create conditions where sensitive information may be compromised, undermining missions, causing adverse publicity, adding to financial uncertainty and raising legal (and regulatory) attention. In such environments, information is often handled by third party transition/test teams with loosely controlled, albeit temporary, access and uncertain accountability.

Organizational and mission integrations such as the Defense Department's Joint Information Environment (JIE), the Intelligence Community Information Technology Enterprise (ICITE) and new agency combinations and expansions (DHA & VA), seek to improve operational effectiveness and realize cost savings by standardizing and consolidating infrastructure. They are motivated further by the desire to adopt common processes and procedures upon an expanded user base. The end result may not pose unmanageable operational security issues, yet the transition itself presents exposures in porting, testing and commissioning the merged infrastructure with particular risk to information assets. In these transitions, database structures, schemas and applications are often from very different cyber environments and perhaps several generations apart. Implementation teams are often composed of unaccountable personnel handling information whose breach or exploitation invites legal and regulatory attention and potentially large financial losses.

Agencies' (and Government contractors') transition to the Cloud seek to realize significant cost savings - both in the ownership of data center assets and the labor associated with its operation and maintenance. Many organizations are intimidated by its uncertain security and reliability, as IT space is shared with large numbers of (often anonymous) users. The cloud is no more or less secure and reliable than turning over IT infrastructure to third-party outsource providers or even captive IT operations. It is in many ways a modern high-speed version of "Time-sharing" from the 1970s and 1980s. Those systems had similar resource sharing and third party control issues, however in the "pre-network" world users had much less fear of security or reliability compromise. Today's FedRamp procedures go a long way toward assuring that Cloud implementations and concomitant security procedures are well thought out – both in the source selection and operation activities. The real risk is not in the end result, but in the transition. The porting of large databases from one implementation to another, the new groups of third parties managing the project, and the personnel and operating procedures for testing and verifying correct operation (often using live mission, agency or personnel data), present uncertain situations where information may be leaked or altered, whether intentionally or inadvertently.

Supply Chain and Counterparty networks, like manufacturers' supply chains and financial relationships, provide significant operational efficiencies and protections yet they may also be exposed to highly impactful risks. The integrity of the parties' deliverable goods and services is not the only risk. The financial fragility of second or third tier providers may invite adversaries' attention. These networks often evolve with hasty and careless testing and validation procedures, exposing entire networks to runaway consequences and future covert channels to multiple parties.

Routine system changes, from database system changes to complete mainframe-distributed system conversions, subject information assets to users and test conditions where accidental or malicious breaches can result from the casual security oversight that often prevails. Special care must be taken during testing for data accuracy, integrity and scalability. There may be considerable risk in using live agency or mission information (data), where new systems and personnel are involved who may expose vital information to breach or exploitation on a large scale.

Mission and National Interests Are at Stake

Operational budget impacts - including resources to monitor threats, secure perimeters, manage identity and handle malware as well as reserves to fund breach response - are a growing part of the cost of doing business. And there are more significant Enterprise or National scale impacts, including loss of Intellectual Property, (Geo)political/public confidence erosion, National Security information leaks and public safety perils.

What Can Be Done?

The vulnerabilities and concomitant consequences attendant to large transformation efforts can be taken out of play. The key is to prioritize them, based upon quantified risk consequence, and then protect the most impactful ones.

- A cyber risk triage process begins by quantifying reputation, mission and financial consequences from lost confidentiality, compromised integrity and lost availability of vital information. The result determines an impact measure which enables executives to manage expenditures commensurate with exposure, and to make prudent risk disclosures to key stakeholders and regulatory bodies. There exist several system engineering approaches to achieving such risk measures.
- High-impact Information Assets may be protected using obfuscation tools to achieve privacy and confidentiality, preserve the integrity and accuracy of testing to validate the correct end state, and minimize legal and regulatory risk. Key to this approach is the distinction between data and information. Hiding or changing data by encryption, masking or de-identification does not achieve the required objective. Obfuscation of the information which represents the data and changing key informational relationships are the basis of assuring that it cannot be reconstructed, implied or reverse engineered. This level of protection preserves the accuracy needed while assuring the privacy sought. There are Information Obfuscation tools which also carry a designation of Qualified Anti-Terrorism Technology (QATT) under the U.S. SAFETY Act of 2002, which provides additional legal protections for provider and user alike.

While organizational and mission transformations can present exploitable vulnerabilities, these vulnerabilities can be measured, isolated and protected by QATT designated tools, mitigating breach occurrences and legal liabilities while reducing the financial and reputation/public confidence consequences.

Sean Singleton Is Managing Director of Oglethorpe Capital, LLC. and a member of New World Technology Partners