The IBIT Report
A Publication of the Institute for Business and Information Technology

David Lanter, Ph.D., GISP, CISA
Director, IT Audit and Cyber-Security Programs
Temple University
Vice President, CDM Smith

Threats & Opportunities in Geographic Information Systems (GIS)

EXPLORING GIS HISTORY, GROWTH, AND SECURITY MANAGEMENT

Fox School of Business
TEMPLE UNIVERSITY®

The IBIT Report

Wyndetryst Print & Web Design
Art Direction, Layout, Editing | wyndetryst.com

 ISSN 1938-1271.

The IBIT Report is a publication for the members of the Fox School's Institute for Business and Information Technology. IBIT reports are written for industry to provide actionable knowledge and are based on rigorous academic research and vendor neutral analysis. Each report focuses on an important cutting edge topic that is of interest to our members.

For additional reports, please visit our website at **http://ibit.temple.edu.**

Disclaimer: The conclusions and statements of this report are solely the work of the authors. They do not represent the opinion of Temple University or the members of the Fox School's Institute for Business and Informational Technology (IBIT).

Review process: IBIT reports are sourced, reviewed, and produced as follows. The managing editor oversees this process. The editor and editor-in-chief consult on topics and identify new sources of reports. The editor typically works with authors who are interested in writing reports and provides feedback on initial drafts. Completed reports are first screened by the editor-in-chief. After approval the report is sent out for review to two members of the editorial board. The editor-in-chief assesses the completed reviews and provides further guidance to authors. Final reports are then professionally produced and made available to IBIT members.

Foreword

Consumer and business use of mobile-device-based location services has become ubiquitous. In the late 1970s it would have been difficult to forecast the evolution of the Canada Geographic Information System (GIS) into the wide variety of innovative ways businesses leverage this technology to improve operations and service customers today.

By 1994 it was clear to the U.S. federal government that there was a critical need to guide the creation of infrastructure to promote geospatial data sharing throughout all levels of government, industry, and academia. However, advanced geolocation technologies also came with risks to privacy and security. What followed was the development of a framework to guide public and private decision-makers in weighing homeland and organizational security implications against the public good of widely available geospatial information.

This *IBIT Report* provides an insightful history of the development of GIS and its related technologies, outlines a framework for classifying sensitive geospatial data based on factors of risk and value, and provides a process for recognizing, governing, and mitigating cybersecurity risks. The approach detailed is applicable not only to location data, but to all data for which there is a cybersecurity concern.

Bruce Fadem
Co-Editor-in-Chief
June 2016

David Schuff
Co-Editor-in-Chief
June 2016

Introduction

Geospatial data produced by geographic information systems (GIS) play a central role in domestic economic and governmental activities. In addition to serving the general public and supporting many federal, state, local, and tribal government activities, geographic data aids in protecting public health and safety and bolsters the progress of science and our ability to compete in international market places.

The National Academy of Public Administration[1] identified GIS data as essential to greater than 50% of the nation's domestic economic activities. The free flow of geographic information between the government and the public is essential to informed public participation in democratic decision-making and private reuse of the public's investment in government information. For this reason, public geospatial data dissemination is central to the missions of many public, private, and non-profit organizations.

In recent years, however, protecting sensitive GIS information for national homeland security reasons has become a concern. In 2011, the U.S. Governmental Accountability Office[2] recognized the lack of enforcement mechanisms for controlling information security risks pertaining to critical national infrastructure, including water supplies, oil and gas pipelines, and electrical transmission networks. **This report explores aspects of the history of GIS, unique opportunities it presents for economic development, and how to effectively handle information security risks associated with public GIS data.**

What is GIS? A **geographic information system (GIS)** is a computer system for capturing, storing, checking, and displaying data related to positions on Earth's surface. **GIS** can show many different kinds of data on one map. This enables people to more easily see, analyze, and understand patterns and relationships.

- National Geographic Society

Executive Summary

Geographic information is a valuable decision-support asset ubiquitously available across desktop, web-based, and mobile platforms and leveraged in private, public, non-profit, and academic sectors of our economy. Recognized as a key component in 80-90% of government data[3], geographic location is a major contributor to informed decision-making and business growth. Much geographic data compiled by our national agencies is readily available over the Internet using the National Spatial Data Infrastructure and National Geospatial Data Clearinghouse, which were created under a presidential executive order[4] by the Federal Geographic Data Committee to provide significant cost savings for data collection and enhanced decision-making.

Publicly shared geographic information detailing locations and make-up of critical infrastructure have recently become a concern, as they may unintentionally fall in the wrong hands and increase risks of terrorism.

THE THREE WAYS TO PROTECT CRITICAL INFRASTRUCTURE

It is crucial that critical infrastructure information be protected through effective

1. **Data classification**
2. **Cartographic generalization** and **access restriction**
3. **Metadata** and **data loss prevention** techniques

WHAT YOU'LL LEARN IN THE REPORT

This report provides executives and information scientists with:

- A brief introduction to the **history** and development of public geospatial data and current **uses in business decision-making.**
- A discussion of how geospatial information can expose entities to **threats.**
- Concrete steps to take to **protect sensitive geospatial data** from expensive and reputation-compromising breaches and attacks.

Key Highlights in the History of GIS

Taking Flight: The Origins of GIS

On an airplane in 1961, Lee Pratt, head of the Canada Land Inventory, lamented to Roger Tomlinson, a stranger sitting in the adjacent seat, about difficulties he was having producing a map cataloging the productive land resources of more than 1 million sq. miles in rural Canada.

Pratt desired a printed map with background geography consisting of terrain, rivers, water bodies, roads, and transportation infrastructure, on which to overlay clear plastic sheets containing locations of available natural resources. His goal was to enable visual analysis of spatial relationships between resources and existing and needed infrastructure for developing the nation and its economy. The estimate of $8 million to produce the map seemed high, and there simply were not enough cartographers in Canada to do the work. Already thinking about applying computers to solve geographic problems, Roger Tomlinson explained how he would approach Pratt's problem and was hired.[5]

In 1963, Tomlinson presented a technical and economic feasibility study, which estimated that $3 million would be required to achieve Pratt's vision with a computerized map overlay and analysis system. He gained funding for his approach and enlisted IBM to help him develop the mainframe-based Canada Geographic Information System (Tomlinson, R.F. 1962, 1963, 1967, and 1968).[6,7,8,9] By the 1970s, Tomlinson's Canada Geographic Information System was operational; it was **the world's first Geographic Information System (GIS).**

KEY DEVELOPMENTS IN THE **HISTORY OF GIS AND CYBERSECURITY**

1990

Federal Geographic Data Committee founded to promote coordinated dissemination of GIS data among government and industry[10]

1993

World Trade Center bombed

1994

President Clinton issues an executive order[4] to Federal Geographic Data Committee to **promote geospatial data sharing** and prevent billions of dollars in duplicated efforts across government agencies to collect GIS data

1996

Clinton signs presidential executive order identifying critical national infrastructure, which could undermine the defense or economic security of the U.S. if attacked

9/11 attacks on World Trade Center and Pentagon, which increase concerns around publicly shared GIS data security

2001

RAND Corporation presents framework[12] for protecting publicly available GIS data (See page 21)

2003

2002

FISMA: Federal Information Security Management Act[11] is passed to protect sensitive, critical infrastructure, data, and systems within the federal government and its partners from terroristic threats

2005

Federal Geographic Data Committee published guidance[13] based on RAND's framework for protecting geospatial data

U.S. Governmental Accountability Office recognized that no enforcement mechanisms exist for controlling information risks pertaining to critical national infrastructure, including water supplies, oil and gas pipelines, and electrical transmission networks[2]

Federal Information Modernization Act of 2014[16] updates FISMA and provides an information security leadership role to the Department of Homeland Security and charges the Office of Management Budget with oversight of federal agency information security policies and practices

2011

2013

Obama issues a Presidential Executive Order to Improve Critical Infrastructure Cybersecurity,[14,15] and Department of Homeland Security identifies 16 critical infrastructure sectors to facilitate public-private cooperation in mitigating threats

2014

2015

Nation's critical infrastructure experienced a 20% increase in cyber incidents in fiscal year 2015 over 2014[17]

Early Industry Applications for GIS in America

The public and private sector applications for GIS multiplied quickly starting in the 1980s, spurred by rapid technological development and the rise of the Internet.

The Use of GIS for Economic Development

By the late 1980s, GIS software originally developed at Harvard and refined at Yale University was applied by Dave Cowen and his University of South Carolina graduate students to identify and rank suitable sites within South Carolina to build a new automobile manufacturing plant. They compiled publicly available population and demographic datasets from the U.S. Census Department depicting the spatial distribution of available workforce across the state (e.g. unemployed high school graduates of working age), derived distances of each place within the state to transportation and utility infrastructure, and determined the availability of land based on parcel ownership. Using a computerized map layering and overlay technique in a "map algebra" equation, the team ranked the sites according to desirability, based on multiple geographical factors. This information formed the basis of a successful proposal presented by South Carolina's State Development Board to BMW.[18] In 1992 BMW used the information to build their largest automobile plant and only U.S. manufacturing facility in the City of Greer, Spartanburg County, South Carolina. **The $2.2 billion plant employs around 10,000 people and is part of the company's global five-plant production network.**

BUILDING A NEW AUTOPLANT

THE CHALLENGE:

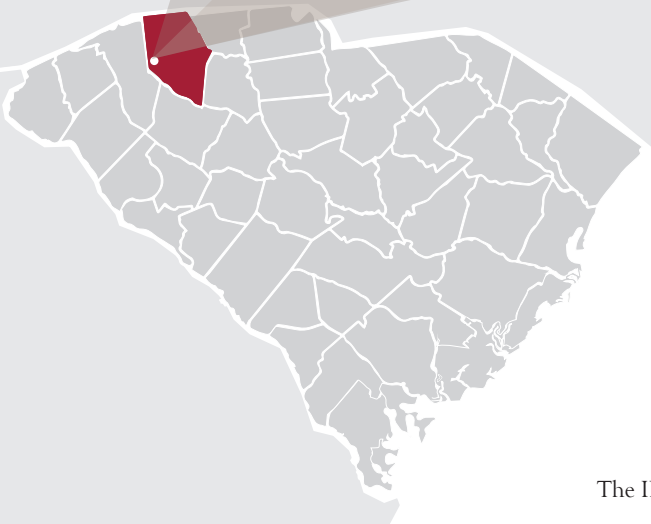
In 1992, the following information was used to choose a location for a new BMW automobile plant using GIS:

- **Distribution of Available Workforce**
- **Distance to Transportation and Utility Infrastructure**
- **Availability of Land**

THE RESULT:

Greer, SC, was chosen for BMW's largest and only U.S. manufacturing facility. As of 2016, the facility

- **Generates $2.2 Billion**
- **Employs 10,000 People**
- **Serves in BMW's Global Five-Point Production Network**



Reusable Governmental GIS Data Themes Readily Available on the Internet include:

Administrative units (e.g. state and county boundaries, tribal land areas, and populated places)

Socio-economic data from the decennial Census and annual American Community Survey

Hydrography (e.g. oceans, seas, lakes, rivers, streams, and watersheds)

Real property (e.g. land-ownership parcels, parks, and reserves)

Transportation (e.g. airports, railroads, roads, and waterways)

The Technological Development of GIS

As the price of disk storage and random access memory dropped and computer processing speed and network throughput increased, the U.S. Geological Survey and Census Bureau produced and made publicly available national GIS datasets containing satellite images and air photography of the earth's surface, land use and land cover maps, street address locations along blocks, decennial census characteristics of populations living in block groups, tracks, counties and states, along with names and locations of populated places and the road networks connecting them. This evolution increased the ability of larger businesses, governmental agencies, and researchers to use geographic data in computers to analyze distributions of people, resources, and hazards and assess suitability of different sites to find best locations for infrastructure and activities.

GIS and the Internet

The Internet not only enabled sharing public GIS data, but it also served as a key platform for launching several innovative business applications based on geospatial technology. In 1990, to promote coordinated development, sharing, and dissemination of geospatial data on a national basis and facilitate use of spatial analysis in decision-making at all levels of government and private industry, the U.S. government formed the interagency Federal Geographic Data Committee (FGDC). Recognizing that geospatial analyses "depend on the availability, quality, and compatibility of digital geographic data" and opportunities existed to save billions of dollars wasted on redundant collection of frequently undocumented and hard-to-find geospatial data stored in incompatible formats, President Clinton signed Executive Order 12906 in 1994.[19] This instructed the Federal Geographic Data Committee to guide creation of a National Spatial Data Infrastructure to "promote geospatial data sharing throughout all levels of government, the private and non-profit sectors, and academia."

In response, the committee created the National Geospatial Data Clearinghouse and guided federal and state agencies in documenting, publishing, and sharing their specialized GIS datasets as "themes" stored on common Internet clearinghouse websites for other agencies and the public to browse, find, download, and reuse as base maps for integrating with their own location-referenced data.

The MapQuest Revolution

Also in 1994, as governmental standards and processes for sharing GIS datasets through the Internet were taking form, R.R. Donnelley and Sons Company launched its free MapQuest website. MapQuest quickly attracted many Internet users by enabling them to use their personal computer browsers to easily find places and addresses on a map and print driving directions of the shortest and quickest routes between origins and destinations.

MAPQUEST'S THREE BASIC GIS FUNCTIONS

MapQuest's web page combined three basic GIS functions with street and road map datasets:

Address Finding or "Geocoding"

Route Finding

Map Display

The result quickly convinced consumers that navigating their computer browsers to the free online map and driving direction website was a better choice than purchasing and installing a CD product for the same information.

Not to be outdone by MapQuest and Microsoft, who followed in providing location search, routing and mapping on the Internet, Google released Google Maps in early 2005. By 2008, Google's Internet web-mapping capability was unified with GPS within Apple's iPhone 3G, and our modern era of handheld mobile and in-car location-based mapping and GIS services for consumers had arrived. Real-time location-based capabilities are now available to users of almost all mobile devices, and a wide range of innovative location-based applications and services are regularly used by businesses and consumers.

Today: Unique Opportunities

Using GIS to analyze the suitability of sites with publicly available data has since become best practice for supporting infrastructure planning within and among national, state, and local government agencies as well as private industry.

It is used in planning improvements, augmentations, and maintenance of transportation networks (e.g. roads, waterways, ports, railroads, and airports), water and sewer systems, school systems, hospital networks, police and fire stations, arenas, and stadiums. GIS analysis helps businesses combine publicly available and private datasets in computational models to support location-based decision-making for capital infrastructure planning, operational logistics, and maintenance management. GIS analysis maps and products help business decision makers plan the locations of many kinds of facilities, including their offices, retail stores, distribution centers, automated teller machines, and IT infrastructure disaster recovery sites. They are also used to identify land to purchase or lease for pipelines (e.g. natural gas, petroleum, and chemicals), electric and communications power lines and networks, cellular phone towers, residential housing developments, and parking lots. Visiongain assessed the 2015 mobile location-based mapping market as generating revenues of $30.56 billion.[20] Juniper Research sees the smartphone and tablet based mobile location based services market growing to $43 billion by 2019.[21]

Today, in addition to driving, walking, and bicycling directions, consumers are using mobile location-based services to find nearby goods and services. Patients are using them to locate pharmacies to fill prescriptions and obtain refills. Businesses and utilities are discovering innovative ways to use them to locate their own assets and resources and service their customers, including guiding prospective customers to nearby wholesale outlets and retail stores. Dispatchers are tracking and rerouting taxis, maintenance personnel, pickups, and deliveries. IT managers are leveraging location capabilities of mobile devices to implement more robust multi-factor physical identity management, and parents are using them to track the whereabouts of their children and be notified when they arrive safely home.

Providing actionable business decision-support information to managers with mobile devices wherever they are is an important emerging trend. For instance, intelligent vending machines participating in "Internet of Things" networks tell distributors their identities, locations, and which products need replenishing. Some distributors in turn are using geospatial data to determine optimal delivery routes for restocking their machines. Others leverage the data to assess sale volumes and identify geographic and demographic patterns to achieve a better mix of products, brands, and vending machine locations. All this increases efficiency and decreases bottom-line expenditures.

Organizations taking advantage of locational references (e.g. addresses, store numbers, asset identifiers, and standardized facility names) within their datasets often combine and spatially overlay them on publicly available and commercially acquired geospatial datasets. The resulting maps provide synoptic overviews and situational awareness that helps managers and decision makers get on the same page and see new opportunities based on relationships, connections, and gaps among geographically distributed assets and resources, existing and prospective customers, distribution centers and transportation networks, and competitors' outlets. Sharing interactive maps of assets, infrastructure, and characteristics of populations they serve (or have yet to reach) can provide new business insights, such as where to expand or contract services based on locations of underserved or over-served market areas.

As businesses improve information sharing and enhance decision-making by making geographic location an explicit integrated part of their enterprise information architectures, it is important to recognize and manage risks to critical infrastructure posed by these non-traditional geospatially enabled IT datasets.

Geospatial Information Containing Potential Threats

While the open availability of GIS data serves essential public and private sector functions, a greater recognition of the threats associated with broad publication has emerged since the mid-1990s.

Three years after the World Trade Center garage bombing of 1993, President Clinton signed an executive order[4] identifying certain infrastructure as vulnerable to attack, explaining:

> *"Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."*

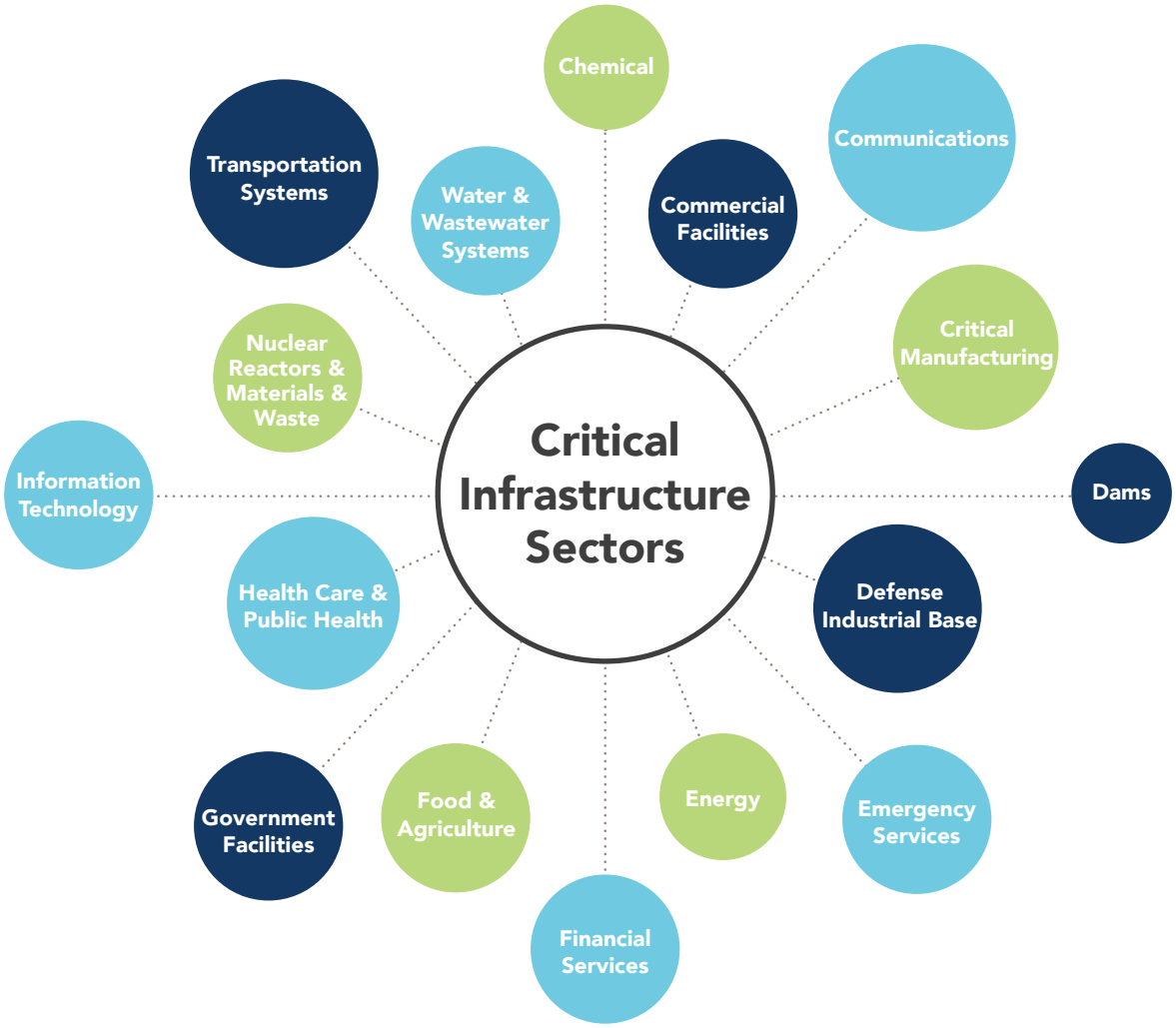
After the bombing of the USS Cole in October 2000 and the terrorist attacks of September 9, 2001, attention focused on protecting critical infrastructure that our country's adversaries might seek to attack. U.S. officials began instituting more policies to protect information and information systems used to plan, operate, and maintain critical infrastructure. It did not take long for GIS data made available through online websites by U.S. governmental and private producers to be recognized as at serious risk of being exploited by those seeking to attack U.S. critical infrastructure and population centers the infrastructure supports.

In 2002, the Office of Management and Budget[22] reaffirmed the federal government's commitment to the Federal Geographic Data Committee's National Spatial Data Infrastructure mission of sharing GIS data via the Internet. To reduce vulnerability of the United States to terrorism, that same year congress passed the Homeland Security Act and the Federal Information Security Management Act (FISMA[1]). The Homeland Security Act defined Critical Infrastructure Information as data able to be used in computer-based or physical attacks against critical infrastructure to threaten public health and safety or harm interstate commerce. The act protected such data from release by the federal government to the public in response to requests made through the Freedom of Information Act. FISMA complemented the Homeland Security Act by requiring federal agencies and any contractors or organizations doing business with them to protect the security of critical infrastructure data and the information systems used to produce, store, maintain, and manage the data's use.

With heightened concerns surrounding data security, the National Imagery and Mapping Agency asked the RAND Corporation to develop a framework to "guide public and private decision makers in weighing homeland security implications related to release of geospatial information." RAND's researchers surveyed public agency websites and found many agencies distributing geospatial information to the public (Baker et al. 2004).[12] They observed that when a diverse range of alternative geospatial data sources useful for identifying targets are widely available, restricting public access creates an inconsequential impediment to attackers. In cases where they found publicly accessible geospatial information useful for identifying and locating potential targets widely available, RAND reported, "…detailed and up-to-date information required for attack planning against a particular target is much less readily available." RAND's analysts pointed out that certain kinds of spatial and temporal data are particularly useful to nefarious actors planning attacks and identified two important kinds of exceptions that should be protected from access and not made publicly available.

HOMELAND SECURITY CRITICAL INFRASTRUCTURE

The U.S. Department of Homeland Security organizes critical infrastructure within sixteen sectors[23] to establish public/private partnerships aimed at increasing communication of threats and facilitate coordination and collaboration in developing and implementing protective risk control measures.

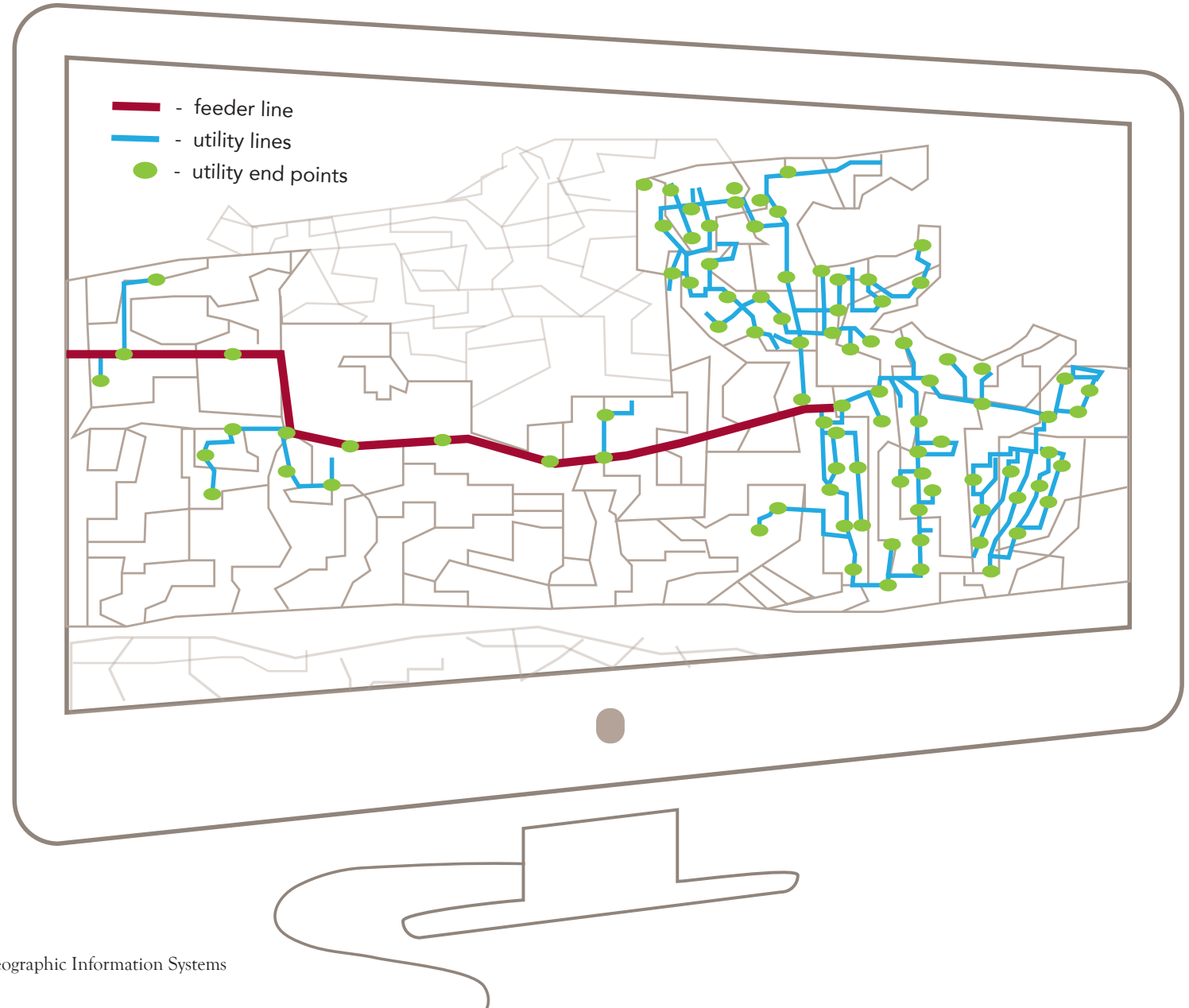


[1] *The Federal Information Security Management Act of 2002 (FISMA) was modernized by the Federal Information Security Modernization Act of 2014 (also called FISMA), which provides a leadership role for the Department of Homeland Security and charged the Office of Management Budget with oversight of federal agency information security policies and practices.*

Infrastructure Vulnerabilities

Geospatial Dataset Map

Locations of vulnerabilities to critical infrastructure not widely known or obvious, such as a choke point in a utility (e.g. water, electricity, gas), telecommunications, or transportation networks are in need of protection. The figure below illustrates a geospatial dataset mapping a fictitious small town's fiber optic Internet and telecommunication network. Notice the town (at the right-side of the figure) is connected via a single green feeder line. This vulnerability provides a communication chokepoint able to cut off the town's citizens and businesses from Internet and voice-over-Internet services, making it impossible for businesses to reach their clients, partners, and Wide Area Network data centers or remote web services.



Data Vulnerabilities

Web-Based Time Charts

Characteristics that change, such as status and schedules of personnel and resources linked to facility locations, may identify high-value assets and times when security vulnerabilities peak. The figure below illustrates a webpage displaying a series of time charts that may be used to find a 'best' time to leverage a vulnerability and breach the facility.

While not all organizations do business in critical infrastructure sectors, the confidentiality, integrity, and availability of many kinds of data are essential to accomplishing the organizational mission and staying in business. The ability to classify the sensitivity of data based on value and risk posed if the data's confidentiality, integrity, or availability is breached must be a core competency. It must be clear which data would benefit the company by being shared publicly, which data need to be protected and only shared within the organization, and which data must have their access further restricted to use only by a limited few. For example, publicly advertising locations of functioning facilities such as outlets and distribution centers can make good sense; however, sharing information about their relative profitability and which ones will be closed and where new ones are being planned likely does not.

Classifying Sensitive Geospatial Data

This section of the report is intended to provide some brief starting points to think through how to operationalize protecting sensitive data.

While severe penalties are in place for breaching protected health information at the federal level and stringent guidelines are enforced regarding reporting corporate financial data, there are no penalties or enforcement mechanisms to protect critical infrastructure information from breaches by non-federal employees in either the Federal Information Security Management Act of 2002 or Federal Information Modernization Act of 2014 (FISMA). As a result, protecting the confidentiality, integrity, and availability of critical infrastructure information is not yet treated as a strategic priority in many businesses and organizations that maintain, improve, and manage public and private infrastructure. Guidance is available in the information security control standards, publications, and processes of the Federal Information Processing Standards, Federal Geographic Data Committee, National Institute of Standards and Technology, and ISACA's COBIT framework.

Managers deciding how to restrict geospatial information can benefit from an analytical framework that helps assess the sensitivity of their organization's geospatial datasets and risk of making them publicly available. According to Federal Information Processing Standard Publication 199, each dataset may be classified, ranked, and labeled with one of three categories based on the potential impact disclosure to an unauthorized person would have on organizational operations, assets, or individuals. [24]

ASSESSING GEOSPATIAL DATA SENSITIVITY

The categories below are recommended by the Federal Information Processing Standard Publication 199:

HIGH	MEDIUM	LOW
Severe or catastrophic adverse effect	Serious adverse effect	Limited adverse effect

To be useful, however, a security framework must take into account the benefits and opportunity costs of restricting public access to the data. Recognizing this, the Federal Geographic Data Committee adopted the RAND Corporation's framework as a basis for guiding decisions about the best approach to assure the security of geospatial information assets.

PROTECTING GEOSPATIAL DATASETS

The framework for protecting geospatial datasets is based on **three factors**:

1

Usefulness in helping attackers identify targets and plan attacks

2

Uniqueness as a source of the information (i.e. if alternative sources are easy to find, then benefits of restricting access to the information may be negligible)

3

Benefits of reducing likelihood of attack by restricting access to data **versus costs** to society accrued by reducing access to using the data for meeting public and private needs

The Federal Geographic Data Committee used Rand's framework in creating Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns [24], which provides procedures that governmental agencies and private businesses can apply in:

- Classifying geospatial data content in terms of homeland security risks
- Selecting and implementing security controls to mitigate the risks of sensitive geospatial data
- Documenting geospatial data security classifications and controls applied to mitigate homeland security risks

While intended for governmental use, these useful procedures can help private, non-profit, and educational organizations think through how to classify their own GIS and location-based data.

According to the guidelines, if the geospatial data do not originate in that organization, then the organization must follow the instructions accompanying the data related to safeguarding them. If the geospatial data do originate in the entity, then the decision concerning whether or not the data need to be safeguarded is based on determinations concerning the three factors described above.

A Guide to Assessing Risk

To assess risk, the guidelines seek answers to the following two questions:

1

Knowledge of the Location

Does knowledge of the location and purpose of a feature as described in the data have the potential to significantly compromise the security of persons, property, or systems?

For example, does the data:

- Provide accurate coordinates for facilities that are not otherwise available and not visible from public locations?
- Provide insights on choke points, which, if used to plan an attack, would increase its effectiveness?
- Aid the choice of a particular mode of attack by helping an adversary analyze a feature to find the best way to cause catastrophic failure?
- Provide relevant current (real-time, near real-time, or very recent) security-related data that are not otherwise available?

2

Specific Features

Does the data identify specific features that render a potential target more vulnerable to attack?

For example, does the data:

- Identify internal features that are critical to the operation of a facility, such as fuel storage at a nuclear reactor or the location of unsecured valves on a major pipeline?
- Provide details on facility layout and vulnerabilities, such as security personnel locations or hazardous material storage areas?
- Provide insights into operational practices, such as shift changes, patrol areas for security personnel, or the times that sensitive operations are performed?
- Provide relevant current (real-time, near real-time, or very recent) vulnerability-related data that are not otherwise available?

YES

If the answer to either question is "yes," there is a risk to security.

How to Remove Risk

The Federal Geographic Data Committee's guidelines instruct the organization to first consider the uniqueness of the data and determine if actions taken to safeguard the information will be effective. If the organization determines the geospatial data under evaluation cannot be obtained by observation or readily available sources (e.g. Google Maps, Bing Maps, Yahoo! Maps, Open Street Map, nationalmap.gov, and data.gov) then the guidelines instruct the agency to evaluate if "the security costs outweigh the societal benefits of active dissemination of the data."

Should the security risks outweigh the benefits of publicly sharing the data, then safeguarding the data can be achieved by either modifying or restricting access to them. If the organization has the authority and believes that changes to the GIS dataset to remove or obscure sensitive information will effectively mitigate the security risk without significantly diminishing the integrity and value of the dataset, then the Federal Geographic Data Committee's security guideline supports the organization's decision to change the data. The process of reducing detail in GIS data while retaining essential geographic characteristics necessary for decision-making is called cartographic generalization. Cartographic generalization applies five data reduction techniques individually or in concert to remove detail from offending geospatial features: selective omission, simplification, combination, exaggeration, and displacement.

If the organization does not have the authority to change the data, or if generalizing the data will undermine its value, then the organization can decide to restrict access to the data.

In addition to assessing the impact a breach in confidentiality can have, organizational entities should assess the impact of losses to data integrity and availability. When choosing between generalizing or restricting access to critical geospatial datasets, business data owners need to evaluate and take into account the effects removing or reducing details from geospatial datasets to protect their confidentiality may have on their organization's operations, assets, or individuals. One pragmatic solution sophisticated data owners can implement to achieve value from their geospatial data while controlling risks is to make alternative versions of the data available to different users. For example, they can provide datasets with sensitive data "for official use only" to internal decision makers and generalized datasets with sensitive elements omitted to external stakeholders.

UNDERSTANDING THE TERMINOLOGY

Cartographic Generalization – In normal map design and production the goal is to preserve truth while deleting and modifying data from a geographic dataset to reduce visual clutter and increase legibility in the resulting map. In security mapping the goal of preserving truth is traded off with mitigating the risk of sharing information that may aid terrorists and other adversaries by removing and modifying data. Techniques of cartographic generalization that can employed to protect geospatial information include:

- **Selective Omission** - Normally uses specific rules that govern decreasing information based on the zoom-level or scale of the map, but in security mapping information is decreased based on security classification and sensitivity of the data.
- **Simplification** - Reduces details in linear features and outlines of areas in a manner that preserves general direction, location, and major elements of shape.
- **Combination, Exaggeration, and Displacement** - To hide specific sensitive geographic features that are nearby others of the same type, selective omission and simplification are often accompanied by combination, exaggeration, and displacement. In combination, isolated features associated with medium and high disclosure impacts are grouped together with adjacent features of lower impact to form a continuous whole. The sensitive features are omitted and the general outline of the resulting area is simplified. When small differences in position are important to the map user, displacement may be applied to keep the remaining features visually distinct and in relatively accurate proximity to adjacent features.

Geospatial Security Metadata & Data Loss Prevention Capabilities

The Federal Geographic Data Committee now uses the International Organization for Standardization's (ISO) Geographic Information Metadata Specification ISO-19115-1:2014 as its standard for documenting GIS datasets.

The resulting metadata records are designed to provide enough information to enable prospective users to determine a dataset's fitness for meeting their uses as well as important security information about the dataset. The Federal Geographic Data Committee's security guidelines recommend including the following information security metadata elements to accompany and inform the access control placed over a geospatial dataset:

- **Abstract** - Overview of potential security concerns, decisions, date made, and safeguards applied
- **Access Constraints** - Restrictions on access to the geospatial data
- **Use Constraints** - Restrictions on user or redistribution of the geospatial data
- **Security Classification System** - Security classification system used to classify the geospatial data
- **Security Classification Level** - Security classification level of the geospatial data
- **Metadata Access Constraints** - Restrictions on access to the metadata describing the geospatial data
- **Metadata Use Constraints** - Restrictions on user or redistribution of the metadata describing the geospatial data
- **Process Step** - Modifications (i.e. generalizations) made to the dataset to safeguard sensitive information
- **Metadata Security Classification System** - Security classification system used to classify the metadata
- **Metadata Security Classification** - Security level of the metadata describing the geospatial data

An organization implementing an information security management system could link this metadata to the corresponding geospatial dataset within its enterprise data architecture and leverage the security information to determine if the data have already been safeguarded through generalization or need to be protected by restricting access or blocking transport within the IT network. Based on ISACA's COBIT 5 Enabling Processes [25], accountability for establishing and maintaining such an information security management system to continuously protect geospatial data belongs to the Chief Information Security Officer (should one exist). Responsibility for developing and leveraging metadata to protect geospatial data assets, in contrast to accountability, can be shared among a small group of individuals: Chief Information Officer, Head of IT Administration, and the Information Security Manager.

To ensure success, however, other individuals and groups should be consulted to gain their guidance for aligning, planning, and organizing the protection of GIS data assets. Depending on the value offered and risks posed by the data a subset of the following should be consulted with:

- Chief Executive Officer
- Chief Operating Officer
- Business Executives
- Strategy Executive Committee
- Chief Risk Officer
- Enterprise Architecture Board
- Enterprise Risk Committee
- Regulatory Compliance
- Audit
- Business Continuity Manager
- Privacy Officer

As a practical matter, COBIT also recommends keeping the following groups and individuals informed about the classification and protection measures applied to the data assets:

- Business Process Owners
- Programs/Projects Steering Committee
- Project Management Office
- Head Information System Architect
- Head of Information System Development
- Head of IT Operations
- IT Service Manager

Including a data loss prevention (DLP) capability within an organization's information security management system would enable data owners to control which datasets can be accessed, transferred, and shared outside the corporate network and which datasets to protect and block from being sent outside the network. Geospatial metadata containing security classification information offer the possibility of implementing business rules within a DLP solution to help assure that unauthorized users cannot maliciously or accidentally share associated geospatial data whose disclosure could put the organization or its critical infrastructure at risk. For example, if a well-intentioned employee attempted to add sensitive geospatial dataset to the organization's publicly facing cloud-based mapping platform, the DLP system would intervene and deny permission to the employee.

7 WAYS TO CREATE AN INFORMATION SECURITY MANAGEMENT SYSTEM

To establish and maintain an information security management system providing formal standardized continuous geospatial information security, while enabling secure technology and business processes, **ISACA's COBIT 5 Enabling Processes suggests seven activities:**

1. Define the boundaries of the information security management system in terms of the IT network, locations, and user groups it supports; systems; and data assets comprising it and residing within it
2. Explain how the information security management system fits within the enterprise's policy and aligns with the enterprise, organization, location, assets, and technology
3. Align the system with the overall approach the enterprise is taking to manage security
4. Obtain management authorization to implement, operate, and modify the information security management system
5. Develop and maintain a statement of applicability that describes the scope of the information security management system
6. Define and communicate information security management roles and their responsibilities
7. Communicate the information management system's approach

Conclusion

The Data Sharing Frontier

Innovations continue to provide us with new kinds of geographic information and spatial decision-support capabilities.

They have helped us realize and move well beyond Bill Gate's 1977 vision for Microsoft: "A computer on every desk, and in every home." Our organizations and businesses can gain increased benefit by leveraging public geospatial datasets, integrating them with corporate datasets in geographic information systems, processing them in spatial analysis models and decision-support applications, and delivering their results via compelling interactive displays on our mobile devices. The results can better inform us about our customers, assets, resources, and opportunities. They can help our organizations make better strategic and tactical decisions. Harvesting value from geographic data, spatial analysis, and location-based technologies, however, comes with the responsibility to recognize, govern, and mitigate cybersecurity risks that accompany them.

In the age of Google mash-ups and ESRI Story Maps, businesses can combine their own data with publicly available data sources and distribute them via mobile and browser-based maps. Due to either inadvertent mistakes or malicious intent, these new geospatial data services must protect against leaking and disclosing sensitive data, such as private or company information, intellectual property, financial or patient information, credit-card data, personally identifying information, or critical national infrastructure information to unauthorized people. Information security projection is especially true in service-oriented enterprise architectures with web-based application program interfaces that provide access to organizational datasets that can be readily linked, combined, and extracted with unintended consequences.

Data loss prevention (DLP) systems are now available that combine data security classification metadata with user identity, data access policy, authorization, and access management capabilities to detect and block access to and distribution of sensitive data by unauthorized users. Integrating DLP systems with data security metadata enabled enterprise data architectures and warehouses offers a way to control the risk of sensitive geographic information being disclosed or leaked by restricting access and distribution, whereas cartographic generalization can be judiciously applied to remove sensitive details of the data to share with the public.

While geospatial data has much potential to help grow businesses, these possibilities also present a strong need to safeguard sensitive information. This report is meant as a first step for understanding a portion of the history of cybersecurity and GIS, its potential, and some means for mitigating GIS-related security risks.

References

[1] National Academy of Public Administration, 1998. Geographic Information for the 21st Century: Building a Strategy for the Nation, Washington

[2] U.S. Government Accountability Office, 2011. Critical Infrastructure Protection – Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use, GAO-12-92

[3] Federal Geographic Data Committee, 2006. How GIS and Mapping Technology Can Save Lives and Protect Property in Post-September 11th America

[4] The White House, 1994. "Executive Order 12906 Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure"

[5] Dempsey, Caitlin 2012. Who Coined the Phrase Geographic Information System, in GIS 101 – Learning GIS

[6] Tomlinson, Roger F. 1962. "Computer Mapping: An Introduction to the use of Electronic Computers In the Storage, Compilation and Assessment of Natural and Economic Data for the Evaluation of Marginal Lands." Report presented to the National Land Capability Inventory Seminar held under the direction of the Agricultural Rehabilitation and Development Administration of the Canada Department of Agriculture, Ottawa

[7] Tomlinson, Roger, 1963. "Feasibility Report of Computer Mapping System." Report to Agricultural Rehabilitation Development Administration, Department of Agriculture, Government of Canada

[8] Tomlinson, Roger F., 1967. "An Introduction to the Geo-Information Systems of the Canada Land Inventory", Department of Forestry and Rural Development, Ottawa

[9] Tomlinson, Roger F., 1968. "A Geographic Information System for Regional Planning" Paper published in unreferenced source by R.F. Tomlinson, Department of Forestry and Rural Development, Government of Canada

[10] Robinson, M. (2002), "Improved Policy for Coordinating the Development of the National Spatial Data Infrastructure", Proceedings of FIG XXII International Congress, Washington, D.C. https://www.fig.net/resources/proceedings/fig_proceedings/fig_2002/Ts3-5/TS3_5_robinson.pdf

[11] Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107–347, 116 Stat. 2899).

[12] Baker, John C. et al. 2004. Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information, RAND National Defense Research Institute

[13] Federal Geographic Data Committee, 2005. Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns

[14] The White House, February 12, 2013, Executive Order - Improving Critical Infrastructure Cybersecurity

[15] Presidential Policy Directive-21 (PPD-21) of February 12, 2013 (Critical Infrastructure Security and Resilience) https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[16] Public Law 113-283, "Federal Information Security Modernization Act of 2014" https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

[17] Kovacs, E. on January 20, 2016, "Critical Infrastructure Incidents Increased in 2015: ICS-CERT", Security Week , http://www.securityweek.com/critical-infrastructure-incidents-increased-2015-ics-cert

[18] South Carolina State Development Board Annual Report 1991-1992. http://dc.statelibrary.sc.gov/bitstream/handle/10827/18759/SDB_Annual_Report_1991-1992.pdf?sequence=1&isAllowed=y

[19] The White House, Executive Order 12906, "Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure", Federal Register Vol. 59, No. 71. April 13, 1994. http://www.archives.gov/federal-register/executive-orders/pdf/12906.pdf

[20] http://www.prnewswire.com/news-releases/mobile-mapping-market-report-2015-2020-driving-value-in-location-based-services-lbs-local-search-geolocation-solomo-gis--spatial-data-300193448.html

[21] http://360.here.com/2015/11/05/digital-mapping-drives-the-mobile-location-based-services-market/

[22] https://www.whitehouse.gov/omb/circulars_a016_rev

[23] https://www.dhs.gov/critical-infrastructure-sectors

[24] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[25] http://www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx

About the Author

David Lanter

David Lanter joins the faculty of Temple University and the Fox School of Business in the Management Information Systems Department as director of the Information Technology and Cyber Security programs. Lanter, a vice president at CDM Smith, routinely leads teams of software engineers, computer scientists, data specialists, and subject matter experts in designing and developing high-performance applications, decision support systems, and enterprise data architectures for public and private sector organizations from the international to the municipal level. A pioneering inventor of data provenance metadata and geospatial data management and quality assurance, Lanter was research director at Rand McNally; a software design engineer at Microsoft, where he led quality assurance for the firm's geography products; and president of Geographic Designs Inc., where he provided commercial off-the-shelf and custom artificial intelligence metadata processing capabilities for helping government agencies and utility and private organizations visualize, derive and analyze big datasets and manage quality in their enterprise geographic information systems. As a systems analyst at Grumman Data Systems he designed and prototyped the first reusable software library to support real-time, near real-time and non-real-time cartographic applications for tactical and strategic systems of the U.S. Airforce. As an assistant professor of Geography at the University of California in Santa Barbara, he taught Geographic Information Systems, cartographic design and production, and applications programming.

Professor Lanter is a Fulbright Scholar, a Research Fellow of the National Center for Geographic Information and Analysis, and a recipient of multiple Values in Action awards from CDM Smith, a Best Scientific Paper in Geographic Information Systems award from the American Society for Photogrammetry and Remote Sensing, and Outstanding Research Award from Sigma Xi Science Honor Society.

He recently graduated with a Master of Science degree in Information Technology Auditing and Cybersecurity from Fox School of Business at Temple University. Professor Lanter's Ph.D. is in Geographic Information Processing from the University of South Carolina, his Master of Arts degree is in Geographic Information Systems from the State University of New York at Buffalo, and his Bachelor of Arts with honors is in Science, Technology, and Society from Clark University, where he won a Von-Laue Research Scholarship Award for his research on nuclear weapons proliferation. He chaired the Urban and Regional Information System Association's (URISA) Workshop Development and Curriculum Development committees, helped start up URISA's Leadership Academy, and recently coauthored: "Geoprocessing, Workflows, and Provenance" in Remote Sensing Handbook: Remotely Sensed Data Characterization, Classification, and Accuracies, and "User Centered Design" in Wiley-AAG's International Encyclopedia of Geography, expected sometime in 2017.

Fox School of Business
TEMPLE UNIVERSITY®