1

NAVIGATING TODAY'S THREAT LANDSCAPE

Introduction

Today's threat landscape is often compared to a high stakes game of whac-a-mole: just as security professionals focus on thwarting one mole-like threat, others are already popping up. Security threats emerge at a dizzying speed and security professionals are often left reeling as the threat landscape changes around them. A vital tool in understanding these changes has been historical threat reporting. Historical threat reports summarize events related to security threats over a fixed period of time. There are legions of historical threat reports available; a Google search for "cyber security threat report" yields over three million results. These reports may cover general cyber security threats or specific focus areas (e.g., web-based applications). There are quarterly threat reports and annual threat reports, but all historical threat reports reflect backwards.

Historical threat reports have the valuable attribute of mapping out the threat landscape as it appeared in the past. And, although many historical threat reports attempt to predict future trends and shifts, they provide only limited visibility into the threat landscapes of today and tomorrow. To combat the threats of today and predict the threats of tomorrow, enterprises need to view their security infrastructure, products and data collection in a different way. Instead of reporting after the fact, threat forecasting looks to prevent security incidents and data breaches before they happen. The exploration of threat forecasting as laid out in this book will give organizations the tools needed to protect themselves in an ever evolving threat landscape. By adopting a

Threat Forecasting. http://dx.doi.org/10.1016/B978-0-12-800006-9.00001-X

policy of threat forecasting, security professionals can stop playing whac-a-mole and begin to know where the next threat is likely to come from.

Why Threat Forecasting

No organization is impervious to security failures. By adopting a systematic approach to threat forecasting, your organization can not only improve your defenses against today's threats, but also form reasonable predictions about the threats of tomorrow. Although, it is true that no threat forecasting approach will be able to predict and stop attacks 100% of the time, when it is carried out correctly and consistently, threat forecasting will increase your organizational efficacy in detecting and preventing attacks. The side effect of preventing attacks is saving your company time, money and the embarrassment of a public data breach.

Threat forecasting allows you to apply real-world threat intelligence to the data collected within your organization to identify patterns or trends "in-the-wild" (i.e., currently active on the Internet) that may impact your organization. Threat forecasting enables your organization to:

- identify knowledge elements within your data for collection for tracking/reporting (refer to Chapter 4—Identifying Knowledge Elements)
- subscribe to threat intelligence feeds to get a holistic view of the greater threat landscape (refer to Chapter 5—Knowledge Sharing and Community Support)
- combine all datasets together and use identified trends to determine high-risk elements and provide protection to vulnerable areas prior to attack/breach (refer to Chapter 6—Data Visualization and Chapter 7—Data Simulation).

Please refer to Chapter 2—Threat Forecasting for more information.

The Effects of a Data Breach

Data breaches are becoming part of our daily lives. Adversaries are better organized than ever and they are likely targeting your company's data. This is not a scare tactic or a way to encourage you to go out and buy a bunch of security equipment. The message we want to convey is that no one is immune and data breaches are almost an inevitable occurrence in today's threat landscape. Malicious threat actors are attacking all industries and are targeting both smaller startups and giant multinational

corporations. As a consequence of these malicious activities, the Incident Response (IR) market has exploded in recent years. By 2017, the IR market is expected to grow into a $14 billion industry.[1]

With costs both tangible and intangible rapidly accumulating in the wake of a data breach, there's no doubt a data breach will cost your organization big bucks. A Ponemon Institute study found that not only have cyber-attacks increased in frequency in recent years but also it is becoming more expensive to address them, with the average data breach costing companies in the study $3.8 million.[2] When remedying a data breach your organization will incur two types of costs: direct and indirect. Direct costs include contracting outside forensic or IR experts, outsourcing customer hotline support, notifying customers (both digitally as well as via mail), providing credit monitoring subscriptions for customers and offering free or discounted future products and services. Although indirect costs can be more difficult to quantify, these costs include internal investigations and communication, customer attrition and weakened customer acquisition rates. Indirect costs represent the harm a data breach can cause to your organization's reputation and the resulting loss of customer trust. Because of the far-reaching impacts, determining how much a data breach could cost you can be tricky; per record cost estimates range from $0.58[3] to $154.[2] The lower end of cost estimates includes only direct costs while the upper end includes both direct and indirect costs. One final note on estimating cost relates to the efficacy of measuring the true impact. Neither model referenced for estimating cost applies to data breaches of over 100,000 records. The total cost of a catastrophic data breach is almost impossible to estimate. Unfortunately, most data breaches that have made the news in recent years have been catastrophic as illustrated in Fig. 1.1.

The lag time between compromise and discovery compounds damages incurred from a data breach. Although attackers are able to overwhelmingly compromise an organization and extract data "within minutes,"[3] it can take days for an organization to discover

[1] Enterprise Incident Response Market Booms to $14bn as Attacks and Threats Multiply, ABI Research, Online, https://www.abiresearch.com/press/enterprise-incident-response-market-booms-to-14bn-/.

[2] 2015 Cost of Data Breach Study: Global Analysis, Ponemon Institute LLC, May 2015, downloadable at https://www-01.ibm.com/marketing/iwm/dre/signup?source=ibm-WW_Security_Services&S_PKG=ov34982&S_TACT=000000NJ&S_OFF_CD=10000253&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US&cm_mc_uid=94450766918914542954680&cm_mc_sid_50200000=1454295468.

[3] Verizon Data Breach Investigations Report, Verizon, online, http://www.verizonenterprise.com/DBIR/.

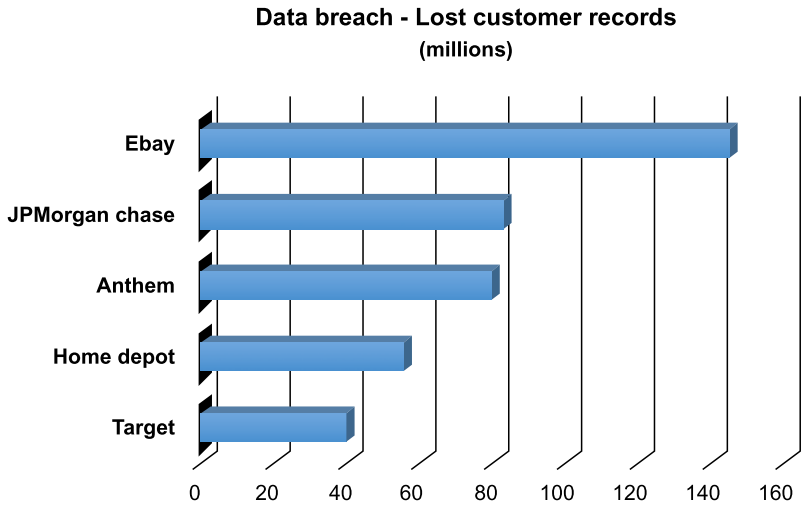

Fig. 1.1 Data breach—lost customer records.

a data breach. In some cases, weeks or months pass before organizations uncover data breaches. In a few extreme examples, data breaches had occurred years before organizational discovery. Following threat forecasting practices will better position your organization to prevent data breaches, and, in addition, when a data breach does occur, threat forecasting practices will enable you to detect the intrusion quickly. But the scope of threat forecasting looks beyond the speed of organizational discovery to the speed of information sharing. It is estimated that "75% of attacks spread from Victim 0 to Victim 1 within one day (24 h)."[3] Sharing knowledge elements, such as indicators of compromise and indicators of interest quickly with applicable platforms, tools and industry groups, can provide real help to likely subsequent victims.

Barriers to Adopting Threat Forecasting Practices

Given the prevalence and cost of data breaches, the need for threat forecasting is obvious. However, many organizations have been reluctant to adopt threat forecasting practices, fearing the costs associated with the required changes. The good news is that threat forecasting relies on a foundation of solid security practices and infrastructure. You may be surprised to discover that your organization has already deployed tools that can be leveraged to begin incorporating a practice of threat forecasting. Moreover, the organizational implementation of threat forecasting practices

lends itself to a phased approach, so changes can be made (and any associated costs incurred) incrementally.

Going Beyond Historical Threat Reporting

As previously mentioned, there is no shortage of historical threat reporting. Many prominent companies including Verizon, HP, IBM, Symantec and McAfee release periodic threat reports. These reports detail trends and changes to the threat landscape over the preceding year, quarter or other specified time period. Although reports are generally jam-packed with useful information, the findings can be perceived as out of date since these reports are typically released sometimes months after the time period they cover. Based on these reports, many organizations will make adjustments to their security policies and procedures by focusing on key areas in the reports they have reviewed as applicable to their infrastructure. Because these reports draw data from the past, they are helpful for understanding yesterday's threat landscape. When looking for guidance on the threat landscape of today and tomorrow, these reports have limited use. When reviewing the information provided in these reports it is helpful to be mindful of their key limitations: timing and generalization.

STRENGTHS OF HISTORICAL THREAT REPORTS

Please don't think we're discounting the usefulness of historical threat reports; they are vital tools for any IT organization or security professional. Because our focus is moving toward a threat forecasting mindset, we've spent time in this chapter establishing a need to look beyond historical threat reports. But make no mistake, historical threat reports often present a wealth of information in an organized and concise manner. They are invaluable tools for understanding the security threat landscape and security trends during the period of time in which they cover.

For more information on the uses of Historical Threat Reports, please refer to Chapter 9.

Timing

Threat forecasting goes beyond historical threat reporting. By accounting for the changing threat landscape in real time, risk is reduced, security attacks can be prevented and infrastructure compromises can be detected earlier. Historical threat reporting on the other hand presents the following three challenges for

organizations attempting to react to today's landscape. They are stale data, nimble adversaries and emerging technology.

- *Stale data*—As noted, by the time historical threat reports are released the data is often stale. Instead of relying on yesterday's data, threat forecasting aims to quickly analyze data in as close to real time as possible. By analyzing data and trends earlier, you reduce your exposure to risk.
- *Nimble adversaries*—Security professionals aren't the only ones reading historical threat reports. Most adversaries will change their tactics, techniques and procedures once they have been identified. While this aspect of timing is intimately related to stale data, it still bears mentioning.
- *Emerging technology*—Historical threat reports cannot adequately account for emerging technology. By comparison, threat forecasting can account for products on the cutting edge of technology. Shifts in the threat landscape are often indicative of new and emerging technologies in the realms of software, web applications or hardware; threat forecasting can make accommodations for these shifts as they occur instead of falling behind the pace of innovation.

Generalization

Nothing is a substitute for analyzing your own data and combining this with the power of global threat intelligence. Security topics commonly covered in historical threat reports are often subject to a great variation and may change from year to year (or whatever the defined cycle is for the authors of the historical threat report). By employing threat forecasting techniques, your organization can move beyond the generalizations found in historical threat reports to define specific threat profiles facing not just your industry but also your organization.

The State of Regulatory Compliance

In spite of the threats posed by cyber-attacks and data breaches, there are few federal cyber security regulations in place. Most regulations that exist are industry or government specific (at the state or federal level). Today's regulations mostly avoid prescribing specific cyber security measures that should be deployed but instead set forth a standard of a "reasonable" level of security. As such it is best to consider regulatory standards as minimum requirements and build up your security infrastructure accordingly. The following discussion of cyber security regulations is

not exhaustive, however is, instead, an overview of selected items we feel currently have the most impact on today's security landscape, standards and best practices. Please thoroughly familiarize yourself with the federal, state and industry-specific regulations impacting your organization.

Industry Specific Guidelines

Although there are relatively few federal cyber security regulations, both the healthcare and the financial sectors are notable because of the established regulations in these industries. If your organization falls into either of these sectors they will be subject to the specified regulatory requirements. Please note that both healthcare and finance are considered critical infrastructures and as such will rely heavily on the National Institute of Standards and Technology (NIST) framework discussed in the next section.

Healthcare Institutions

The healthcare industry and its associated institutions are primarily regulated by the guidelines defined in the Health Insurance Portability and Accountability Act (HIPAA) that was passed in 1996. Prior to HIPAA being enacted, there was basically no generally accepted security standard nor was there any general requirements for the protection of health information. It is comprised of multiple sections, or rules, that must be followed in order to remain in compliance. The rule that we would like to discuss is the Security Rule, as it provides the governance with respect to technology and the protection of electronic protected health information (e-PHI). According to the HIPAA Security Rule Summary,[4] the Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. Specifically, covered entities must:

- ensure the confidentiality, integrity, and availability of all e-PHI created, received, maintained or transmitted
- identify and protect against reasonably anticipated threats to the security or integrity of protected information
- protect against reasonably anticipated, impermissible uses or disclosures of e-PHI
- ensure compliance to the HIPAA Security Rule of all employees.

[4] Summary of the HIPAA Security Rule, Office for Civil Rights Headquarters—U.S. Department of Health & Human Services, Online, http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

The Security Rule defines "confidentiality" as meaning that e-PHI is not to be made available or disclosed to anyone unauthorized to access it and it follows the definition of "confidentiality" as outlined in the HIPAA Privacy Rule. The Security Rule also defines several other key areas that must be considered while operating within the healthcare industry including:

- *Risk Analysis and Management*—Performing regular risk analysis as part of the defined security management process
- *Administrative Safeguards*—Designating an official security officer, putting in place the proper security management process to oversee items like risk analysis and performing regular workforce training
- *Physical Safeguards*—Securing facility access as well as access to workstations and devices that may have access to e-PHI
- *Technical Safeguards*—Having proper access control, auditability, integrity controls and secure transmissions when accessing e-PHI
- *Policies and Procedures and Documentation Requirement*—Adopting reasonable and appropriate policies to comply with all requirements of the Security Rule as well as maintaining a defined document retention policy.

To dive more deeply into HIPAA, please refer to the Health Information Privacy section of the U.S. Department of Health & Human Services website (http://www.hhs.gov/hipaa).

Financial Institutions

The financial industry is subject to a number of different regulatory requirements. A patchwork quilt of regulation exists because the regulatory environment has evolved over several decades. This patchwork nature of legislation can make navigating the regulatory environment challenging for financial institutions. New legislation often not only sets forth added regulatory requirements, but also amends and updates previous legislation and regulatory requirements. The Center for Strategic and International Studies has released a report that covers the evolution of the financial industry regulatory environment in depth; we recommend this report for those interested in a more detailed picture than the one provided in this chapter. [5]

[5] The Evolution of Cybersecurity Requirements for the U.S. Financial Industry, D. Zheng, Center for Strategic & International Studies, Online, http://csis.org/publication/evolution-cybersecurity-requirements-us-financial-industry.

Most of the regulations we will reference in this chapter do not explicitly spell out cyber security requirements. Instead these regulations require organizations to implement "information security systems" for various purposes (e.g., consumer data protection, identity theft protection and reporting requirements). As legislation has been updated and amended over the years, the meaning of "information security systems" has evolved in an attempt to address the needs of today's cyber security environment. Table 1.1 below provides a summary of some legislation pertinent to our discussion; it is not meant to be an exhaustive list.

Table 1.1 Sample Financial Regulations Overview

Legislation	Description
Bank Secrecy Act of 1970 (BSA)	The BSA was designed to combat money laundering, terrorist financing and tax evasion. The BSA implements reporting requirements and processes for defined "suspicious activity." As technology has advanced, new categories of suspicious activity have been added (i.e., electronic intrusion and account takeover.). Advancing technology has also facilitated more efficient reporting processes
Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA)	The FDICIA was passed at the height of the Savings and Loans Crisis. As it relates to our discussion, the FDICIA focused on operational assurance and transaction monitoring, requiring organizations to implement information security systems
Gramm-Leach Bliley Act of 1999 (GLBA)	The GLBA was perhaps the first legislation to address concerns emerging in the Internet age. The GLBA introduced security requirements designed to protect consumers' personal data. It also mandated a written information security plan. Additionally, the GLBA requires annual information security training for employees. In 2001, the Federal Trade Commission issued guidelines for GLBA implementation and included specific computer security measures such as using multiple layers of access control, implementing controls to prevent and detect malicious code and monitoring network activity to identify policy violations and suspicious behavior
Fair and Accurate Credit Transactions Act of 2003 (FACTA)	FACTA was a response to the widespread problem of identity theft and focused on information security standards to prevent and combat identity theft

In part because of the lack of specificity in many regulations, financial institutions often turn to the guidance, standards and frameworks provided by outside organizations. Regulatory

authorities have found that 90% of financial institutions examined used one or more of these frameworks or standards.[6] We will discuss two of these (PCI DSS and NIST) in the next section, Best Practices, Standards and Framework.

Cyber Security Information Sharing Legislation: Watch this Space

Of course, as the cyber security landscape continues to change, so too will the regulatory landscape. For example, the Cybersecurity Information Sharing Act (CISA) is a bill newly enacted at the time of this writing. The CISA seeks to facilitate information sharing between the government and private companies: "In essence, the law allows companies to directly share information with the Department of Defense (DoD) (including the National Security Agency (NSA)) without fear of being sued."[7] Time is needed before the impact of information sharing legislation can be assessed, but individuals within the information technology and information security community should keep abreast of this and other legislative efforts as they emerge.

Best Practices, Standards, and Frameworks

Because the regulations that do exist mostly avoid prescribing specific cyber security measures, organizations have turned to security standards and frameworks. These provide templates upon which organizations can model their cyber security programs. These standards and frameworks help an organization build a solid foundation of cyber security practices. Following these guidelines will help an organization meet the "reasonable" standard set forth in the few existing federal guidelines. However, to effectively engage in threat forecasting, we believe organizations treat these guidelines as just that. They provide guidance, but you often must add to your cyber security infrastructure and practices in order to reap the benefits of threat forecasting.

[6]Report on Cybersecurity Practices, Financial Industry Regulatory Authority, Online, https://www.finra.org/sites/default/files/p602363 Report on Cybersecurity Practices_0.pdf.
[7]The controversial 'surveillance' act Obama just signed, CNBC, LLC, Online, http://www.cnbc.com/2015/12/22/the-controversial-surveillance-act-obama-just-signed.html.

PCI DSS

First published in May 2009, the Payment Card Industry Data Security Standards (PCI DSS) establishes guidelines for "all merchants and organizations that store, process or transmit" [8] payment card data. Because of the prevalent use of payment cards, these standards reach industries far beyond the financial sector. Although not mandated by federal regulations, compliance with PCI DSS is nonetheless important. Mandatory compliance is established and enforced by major payment card brands. The PCI DSS establishes data security standards for merchants and card processors (see Table 1.2) and outlines an ongoing process of PCI DSS compliance.

If an organization accepts or processes payment cards, it must comply with PCI DSS. The PCI security standards establish reasonable goals for organizations dealing with payment cards and actions required to meet those goals. These goals and requirements are set forth as common sense steps an organization must

Table 1.2 PCI DSS Requirements

Goal	PCI DSS Requirements
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security

[8] Document Library, PCI Security Standards Council, Online, https://www.pcisecuritystandards.org/document_library.

take in order to establish a reasonable level of security. As previously noted, these requirements are a starting point and should be viewed as necessary but not sufficient in organizations striving to build a robust security environment. Table 1.2 summarizes the established goals and requirements.

In order to maintain PCI DSS compliance, the Standards require an ongoing three step process and provide Independent Qualified Security Assessors to monitor and validate compliance. Although the PCI DSS sets overarching industry standards, each major payment card brand maintains its own compliance program. The three step process established by the PCI DSS is in line with cyber security best practices and requires organizations to take steps to assess, remediate and report on their card processing cyber security environments on an ongoing basis (Fig. 1.2). Affected organizations must *assess* their payment card transaction environments, examining cyber security infrastructure, policies and procedure for vulnerabilities. As identified, steps must be taken to *remediate* vulnerabilities. Necessary *reports* must then be compiled to document vulnerabilities identified and steps taken to remediate. As noted, these steps are ongoing, and organizations are expected to incorporate these three steps into their cyber security and IT practices regularly.

Fig. 1.2 PCI DSS three step process.

NIST Cyber Security Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) was created specifically to strengthen protection for companies classified as critical infrastructure, however the CSF's sphere of influence has quickly expanded. Organizations beyond those classified as critical infrastructure have also been looking to the CSF for guidance. Although compliance with the CSF standards is voluntary, it has emerged as the standard against which organizations are judged after a data breach occurs.

The CSF is organized into five core functions: Identify, Protect, Detect, Respond, and Recover. These core functions are then further branched into several tiers "which describe the level of sophistication and rigor an organization employs in applying its cyber security practices."[9] Much has been written about the CSF, its core functions and organizational impacts, so we won't dive too deeply into the framework. Please familiarize yourself with these standards as they apply to your organization. When you begin the process of implementing threat forecasting practices in your organization (explained in Chapter 9), the NIST CSF may be a useful starting point when implementing phase one and evaluating your organization's current cyber security practices, policies and procedures.

Defense in Depth

We strongly believe that defense in depth is the correct deployment strategy for any organization. While it may be more convenient to have a single appliance solution from a deployment standpoint, no single appliance is capable of successfully facing all security challenges. Furthermore, we recommend a blended security vendor environment within your infrastructure. Deploying a single vendor environment, even if it is multiple products from that security vendor, only allows you to benefit from one research team. Deploying a blended vendor environment gives you access to multiple research teams who may have access to different attack vectors (i.e., different research data) and thus provides better security coverage. In our book *Blackhatonomics*,[10] we discuss defense in depth in terms of tier 1 and tier 2 technologies. Especially in large corporations, these are the basic building blocks, in the form of tools and technologies, for building a security infrastructure.

Tier 1 Security Technologies

According to current best practices and regulations, the following tier 1 technologies are considered "need to have" when building out a reasonably secure infrastructure:

- Firewall or next-generation firewall
- Desktop anti-virus

[9] Understanding NIST's Cybersecurity Framework, C. Thomas, Tenable Network Security, https://www.tenable.com/blog/understanding-nist-s-cybersecurity-framework.

[10] Blackhatonomics, Chapter 7, W. Gragido, Syngress, 05 December 2012, http://store.elsevier.com/product.jsp?isbn=9781597497404.

- Secure web gateway
- Messaging security
- Intrusion detection/prevention systems
- Encryption (in transit or at rest)
- Security information event management.

Tier 2 Security Technologies

Tier 2 security technologies are often considered "nice to have" when building out a security infrastructure. These technologies are used by organizations with more sophisticated security infrastructures. They are also often purchased by organizations in the aftermath of a major security data breach. Building an infrastructure that combines tier 1 and tier 2 security technologies provides the most robust risk protection. Tier 2 technologies include:

- Advanced threat detection
- Network and desktop forensics
- Network and desktop data leakage protection
- Behavioral-based analysis
- Security/threat intelligence feeds
- Threat forecasting and modeling.

Update and Evaluate Security Products and Technologies

Do not focus myopically on new security vulnerabilities. IT and security teams can display very reactionary behavior when it comes to new vulnerabilities and it is our opinion that you should understand your infrastructure and its potential weaknesses as opposed to reacting to every new announcement (though note we are not saying it is not important to stay abreast of new threats). The Verizon 2015 Data Breach Investigations Report (DBIR) found that when attacks exploit a known vulnerability, "99.9% of the exploited vulnerabilities had been compromised more than a year after the associated common vulnerabilities and exposures (CVE) was published."[3] This highlights the need for organizations to develop thoughtful policies and procedures for installing patches and updates on existing infrastructure (both endpoints and network devices). Organizations that do not keep abreast of release notes and update devices accordingly are at greater risk of a data breach.

Cyber Security and the Human Factor

No discussion of security best practices can be considered complete without factoring in employee behavior. From phishing scams to social engineering, your employees are likely your largest security vulnerability. We believe every employee should be security-minded. Although turning your employees from security liabilities to champions requires organizational effort, a thorough (and engaging) training effort can pay dividends. The Target data breach is believed to be associated with the successful social engineering of one of Target's suppliers. For more information on this data breach, please refer to Chapter 9 (Connecting the Dots).

Today's Information Assurance Needs

Increasingly, organizations are managing information systems and information-related risks with the same thoughtfulness applied to more traditional systems (i.e., computer systems and networks). This practice is known as information assurance (IA). IA experts "seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and nonrepudiation." Essentially, "IA is the process of ensuring that authorized users have access to authorized information at the authorized time."[11] Meeting IA needs today requires the ability to mesh regulatory requirements, best practices and infrastructure needs with a view towards the security landscape of today and tomorrow. By deploying threat forecasting techniques within your organization, you will undoubtedly enhance the security position of your organization. Because the last thing you want to do is invoke your IR plan, threat forecasting helps you head off the next threat.

Welcome to threat forecasting.

[11] Iowa State University Information Assurance Center, http://www.iac.iastate.edu/.