White Paper

Outbreak: Avoiding Information Security Catastrophes in Cable

Information Security is critically important to the cable industry. Recent embarrassing incidents bring home the consequences of not giving information security the attention it deserves. Yet, by most accounts, the attention given to security is not all it could be. What risks are still out there and what can be done to mitigate them? What would a cohesive, enterprise-wide security strategy look like and what practical steps can a cable security manager take to avoid a security nightmare? This paper proposes just such a nightmare scenario and looks at what can and should be done to prevent scenarios like it from becoming reality.
INTRODUCTION

The initial reports coming into the enterprise security office at All-American Cable Company seemed innocuous enough. Isolated instances of subscribers getting free service are not that uncommon. Customer service agents sometimes make mistakes.

As the few instances became a few dozen and then a few hundred, it was obvious that something was wrong. Director of enterprise security, Dirk Stalwart launched an immediate audit. What that audit found brought a knot to his stomach. Tens of thousands of credit card numbers that had been recorded for purchases of services and content had been canceled and updated. All-American had received hundreds of complaints about increases in SPAM and phone calls from scam artists. The number of calls into customer care complaining about extra charges on bills had jumped through the roof in just the past month.

Dirk’s greatest fear had been realized. The consequences were not good: the headlines in the Wall Street Journal, the mud-dragging in the blogs and, worst of all, the congressional hearings that All-American’s CEO might now have to face regarding what was starting to look like one of the worst security breaches in the history of the cable industry.

But what went wrong? Where should Dirk’s team begin to look for the breach? Where are the vulnerabilities? How were they be exploited? And, most importantly, what steps should they have taken, and should other cable companies now take, to prevent this catastrophic outcome?

All-American had always taken security seriously, working in concert with engineering teams to ensure that its products were built with network security in mind. Yet, there were obviously still weak links in the chain.

How did the credit card numbers get out? They are encrypted and stored in the billing systems. CSRs do not have access to numbers once they are entered. Backups are archived in a secure facility. Transmission of information to the payment processor uses a process conforming to Payment Card Industry (PCI) security standards and others.
What about the phone numbers and email addresses? The security around those is not quite as tight. They are stored in databases and access to them is restricted to a few administrators, though, with the right user name and password, CSRs or even internet users could find this information a piece at a time. But that would not explain the sudden torrent of SPAM and junk mail.

Then there were the complaints about billing problems. Somehow, service codes had been added to subscribers’ accounts without their request. A disgruntled CSR could certainly do this, but in this quantity, and simultaneously with all the other incidents? It seemed pretty unlikely.

The first thing his team noticed was how little people seemed to really know about where all their data resided. For instance, most agreed that credit card numbers are only stored in the billing systems. However the reporting group noted that there was a nightly dump of all billing data into a relational database that they use to generate marketing reports. Yes that data is also reasonably secure but the teams responsible for the reports have full access. The data they were reporting on was not terribly sensitive, but because the data was stored without concern for what was actually needed, an unnecessary vulnerability was introduced. It turned out that “it’s in the billing systems” is a little vaguer than most realized.

A critical first task in ensuring subscriber privacy is data categorization, or the practice of determining how sensitive each bit of data is.
or employees are provided the highest level of security control. This is a multifaceted, risk based activity that involves management and the operational personnel with the company. After this categorization has been completed, a selection of appropriate security controls should be identified to ensure security control baselines were met.

Privacy-related information—data elements that, either singly or in combination with other data, pertain to an individual—must be classified in the most secure category. Organizations may designate this category as “Secret,” “Personally Identifiable Information,” “Restricted,” “Confidential,” “Sensitive,” or by a similarly descriptive label. Information that should be included in this most secure category include name, address, phone number and, most certainly, credit card numbers. In addition, a written policy explaining the various kinds of data included within the classification and accompanied by easily comprehensible examples, should be developed and published for internal organizational use. The security department will contribute to the formulation of this policy, although the actual document may be authored by the legal department, compliance, or a similar control function. The policy should be accessible to all employees to aid in understanding what types of data may fall in this classification category.

This clearly had not occurred at All-American. There was no internal agreement on what data was sensitive and what was not. Subscriber passwords are stored encrypted to minimize the risk of unauthorized access but nobody had thought to guard against a mass release of email addresses and phone numbers. There was, in fact, no policy about the relative sensitivity of different data elements or what level of risk mitigation was appropriate for all of it.

The most surprising discovery, though, was about physical security. Security at the corporate buildings was sufficient but large cable companies are very distributed entities with buildings and head ends that are controlled by autonomous markets. The networks run through these buildings, obviously, as CSRs and technicians need the networks to access billing and other systems. Major portions of billing data were discovered to be located in the head ends to support entitlement of video services. Credit card data was not among it, fortunately, but

Attacks can come from insiders, exposed VPN clients, unsupervised consultants, rogue wireless connections and other threats.
account numbers and service codes were available, unencrypted, in systems that, in some cases, were found to be accessible by giving a confident smile to a cooperative receptionist.

**CORPORATE INFRASTRUCTURE – THE WEAKEST LINK**

Looking deeper, we see that basic network topology is changing rapidly. Traditionally, security has been handled by putting a “hard shell” on the perimeter of the network like a moat around a castle. This perimeter-focused approach to security was based on the premise that if you could keep the bad guys out and only let the good guys in, the core of the network would be safe.

However the definition of what and where the perimeter starts and stops is changing. Employees are becoming more mobile. The network is opened up to off-site business partners. Mergers and acquisitions bring new individuals and technologies into the network.

This crumbling perimeter makes it extremely difficult for companies to define their network assets at any given moment. Attacks can come from insiders, exposed VPN clients, unsupervised consultants, rogue wireless connections and other threats. These new access methods, compounded by the need to maintain accurate reports on and effective control over network assets make perimeter security by itself obsolete.
Adding further complexity, the business is ramping up Web-based customer transactions that need to be wrapped around the internal business applications. These applications hold private customer data such as names, date of birth, and credit card or billing data. This requires companies to overlay a Security Governance model in how they define data and what security measures they place around the applications processing that data.

**LOOKING AT THE PROBLEM**

Because of All-American’s geographic reach, Dirk and his team had the daunting task of understanding where and how the data was categorized internally and managed within their own enterprise. Most enterprises have thousands of devices connected to the Internet (sometimes as many as three to four devices per employee), hundreds of applications installed on the network and gigabits of traffic flowing over the internet each day. The proliferation of wireless access points and the extension of corporate networks to business partners poses another challenge.

As a public company, All-American is also required to provide proof of compliance with the Sarbanes-Oxley act of 2002 (SOX) which is facilitated through more rigorous segregation of roles and responsibilities to limit the access that any individual in the organization has.
Dirk must understand the links of each of All-America’s critical security processes and how they interact internally. He discovered that All-American recently contracted with a new billing company. His team was not aware of the change and did not complete a risk analysis to ensure that security would encompass the new billing systems. Given the opportunity, he would have overlapped the organization’s IT Security Governance structure to secure data in accordance with its categorization as per ISO 17799, ISO 27002 and other best-of-industry security standards.

As is common in the industry, All-American Cable Company follows a decentralized model for security compliance. This means that security department managers have policy development and oversight responsibilities for the information security program, but not over the operating units’ information security programs such as the new billing program just established.

Alternatively, a centralized model could have been used so that the department of the CIO or, in some instances, the security department manager would have line-item budget control over all information security activities throughout the department and be responsible for ensuring implementation and monitoring of information security controls throughout the entire organization.

In addition, a centralized model addresses the interconnection of information systems by establishing formal agreements that specify technical and security requirements, defines the responsibilities of the participating departments, and specifies the rules governing them. When these interconnections are properly managed, the added benefits include greater efficiency, centralized access to data, and greater functionality.

The security controls of each of the interconnected systems should be evaluated against the requirements of each of those systems to ensure that the selected security controls are appropriate for the particular interconnection and type of data being processed.
WHERE TO START

What All-American Cable Company discovered is not unusual. Cable companies operate in a fast-moving and competitive industry that always seeks to balance enterprise requirements against time to market. Information Security is one of those tradeoffs and without disasters like the one that All-American faced, its complexity and importance is not always that clear.

Cable companies, like most large organizations, have security and business continuity systems and processes in place, which have grown over time. These systems and processes tend to be influenced by a negative perception of security among different function owners. As a result, security systems have become expensive to maintain, inconsistent across the organization and not fully compliant with best practices. The dynamic nature of the forces that affect these programs means that organizations need an effective strategic planning process.

This process begins by defining the regulations and requirements for data service providers, transaction processors, and business partners. These regulations and requirements can be delivered as part of a broader organizational compliance model initiative like Control Objectives for Information and related Technology (COBIT) or the Information Technology Information Library (ITIL). Next steps would include:

- Development of practical responses to security and privacy challenges
- Prioritization of near- and long-term security strategies and objectives
- Effective communication of strategic decisions through the creation or modification of organizational policies

A COMPREHENSIVE STRATEGY

Developing a comprehensive security strategy can be a challenge but doing so is essential if an organization is committed to protecting subscriber data, conforming to regulatory requirements and protecting its assets. The organization must address a broad range of subscriber information security challenges, including alignment of security to the business risk profile, and reduction of cost and
There are key components to this strategy:

- **Information Risk Assessment** provides a systematic overview of enterprise security capabilities and a roadmap for remediation by assessing governance, policy, data protection, authentication, access, and other security controls.

- **Information Security Program Development** aligns an enterprise security posture with business objectives and helps meet requirements for regulatory compliance by providing guidance to improve the maturity of security capabilities, policies, organization, and controls.

- **Information Security Policy Development** helps ensure compliance with internal and external mandates by defining and mapping policies to best practices, business requirements, and appropriate regulations.

- **Classification for Information Security** provides the basis for the implementation of appropriate security controls by cataloging and identifying the value, sensitivity, and protection requirements of critical business information.

Adoption of a centralized model for IT and Information Security involves specific steps. This process determines the extent to
which the security controls in the information system are implemented correctly, operating as intended, and producing the desired system security posture. It also identifies specific actions taken or planned to correct security control deficiencies and to reduce or eliminate known system vulnerabilities. Finally, it looks at information systems and the controls around them and validates that IT security policy and policy management do not have exceptions.

Adopting a centralized model involves the following items:

- **System Security Plan**
  - Overview of the security requirements, the agreed upon security controls, and supporting security related documents

- **Security Assessment Report**
  - Security controls for logical and physical needs to protect systems and data

- **Risk Mitigation Strategy**
  - Measures implemented or planned to correct deficiencies and to reduce or eliminate known vulnerabilities

- **A system security plan** provides an overview of the security requirements for the information systems and explains the measures taken or planned to comply with those requirements and any interconnection agreements.

- **A security assessment report (SAR)** summarizes the results of the activities undertaken by a certification agent. The security assessment report can also contain a list of recommended corrective actions and the completed system reporting form.

- **A risk mitigation strategy** describes the measures that have been implemented or planned to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known system vulnerabilities.
FINDING A BALANCE

Achieving compliance with information security laws, regulations, standards, and guidance is imperative for an effective information security program. To be successful, management needs to understand how to systematically recognize and address information security risks and take steps to understand and manage these risks through their information security program. Information security should be closely aligned with business or mission goals. The cost of protecting information and information assets should not exceed the value of the assets. To properly align business risks and information security, executive organizational management should facilitate a cooperative discussion between business units and information security managers.

Information security program implementations often suffer from inadequate resources—management commitment, time, money, or expertise. By understanding the benefits of meeting compliance objectives, an organization can overcome these obstacles and appreciate the gains achieved through implementing effective security practices. Investment in information security has many benefits. These benefits include:

- **Business success/resilience.** Effective security ensures that vital services are delivered under all operating conditions. Information is one of the most important assets to an organization. Ensuring the confidentiality, integrity, and availability of this strategic asset allows organizations to carry out their missions.

- **Increased public confidence and trust.** Proactively addressing security can be used to build positive public relations – communicating to constituents the organization’s focus and priority on protecting their sensitive information.

- **Performance improvements and more effective financial management.** Specific performance gains and financial savings are realized by building security into systems as they are developed, rather than adding controls after the systems are operational—or in a worst case, after there has been a security breach or incident.
• Executive accountability. Corporate executives may face administrative and/or legal actions for not complying with security mandates.

• Improved ability to deliver products and services electronically. Effective security provides the integrity and availability necessary to meet demanding customer service requirements.

• Mature and integrated risk management processes. The principal goal of any risk management process is to protect the organization and its ability to perform its mission, not just its information assets. Therefore, the risk management process should be treated as an essential management function of the organization, rather than a technical function carried out by system administrators.

KEYS TO SUCCESS
Implementing a robust information security program within a cable company is challenging. Management has to contend with constantly changing technology, multiple compliance requirements, increasing complexity of information security, and changing threats. However, management can navigate these challenges and accomplish critical information security goals. There are some keys to success:

• Strong leadership is the foundation to build a successful information security program
• Good business practices lead to good security
• A proactive approach avoids surprises
• It is critical to develop stakeholders and support within the executive ranks and focus their efforts on collaboration and cooperation
• People can make or break your program
• Information security program development is comprehensive and takes time to accomplish

CONCLUSION
All-American’s valiant security director may never know exactly who was responsible for their security breach or how. There were several areas where a breach was possible and, ultimately,
even likely at some point. What matters, though, for All-American and more importantly, for other cable companies, is that the likelihood of future breaches can be greatly reduced by undertaking a review of current security practices, mapping your data through the various business functions responsible for it, assessing your risk and developing a cohesive policy.

Over time, information security efforts may need to be revisited because of changes in the corporate mission, operational requirements, threats, environment, or deterioration in the degree of compliance. Periodic assessments and reports on activities can be a valuable means of identifying areas of noncompliance. Reminding employees of their responsibilities and demonstrating management’s commitment to the security program is key to maintaining effective security within the constantly changing information security environment. Management should ensure a life-cycle approach to compliance by monitoring the status of their programs to ensure that:

- Ongoing information security activities are providing appropriate support to the company mission
- Policies and procedures are current
- Security controls are accomplishing their intended purpose

An initial security assessment is the first step on a path that can keep your business out of the headlines.
About the Author

Chris Devlin, a director at pureIntegration leads Security & Privacy engagements for our Federal and commercial clients and provides thought leadership in the security community and Federal industry for the company. Chris has spent over 21+ years as a trusted and recognized subject matter expert in the management of logical and physical system integration by applying IT governance modeling using FISMA, NIST, NIACAP, DIACAP and DCID. He comes from a background as an Executive Consultant in leading top fortune 500 companies with a founded intellectual knowledge base as a former Central Intelligence Agency Security Manager. He is a member of the Global IT Security Consortium Community, Advanced Technology for Airport Security (ATAS) Group, and Port Security Council and is a published speaker on security integration from a service oriented architecture governance approach and concept for C&A. He also holds certifications as a:

- Information Security Auditor (CISA)
- Information Security Manager (CISM)
- Information Technology Infrastructure Library (ITIL) Best Practices
- Certified Protection Professional (CPP)
- International Organization Standards (ISO) Implementation BS17799/27001
- Technical Surveillance Countermeasures (TSCM)
- Institute of Electrical and Electronics Engineers (IEEE)

Chris can be contacted at Chris.devlin@pureintegration.com

About pureIntegration

pureIntegration is a systems integration company with a track record of achieving measurable business results. With our deep industry expertise, we give our customers a competitive edge with bold solutions to their critical business problems. pureIntegration’s differentiated approach strives to exceed service and delivery expectations through our proven methodologies, focus on innovation, partnership with client teams, and unmatched resources. For more information, visit www.pureintegration.com or call 703-707-9680.