Case Study – Canadian Utility

Security-as-a-Service (SECaaS)

This document illustrates the benefits and advantages realized by one of Ontario's Local Distribution Companies (LDCs) who selected Stratejm's Security-as-a-Service to enhance their enterprise security and risk posture.

Office: 888.876.0504

Email: info@stratejm.com

Website: www.stratejm.com

About This Case Study

Ontario's Local Distribution Companies (herein LDCs) are responsible for the reliable distribution of electricity to customers in their designated marketplace and territory. As with any utility, significant capital investments have been made in Operations Technology (OT), and, to a lesser extent, in Information Technology (IT) to deliver services reliably, securely and efficiently. OT has traditionally been walled off and kept separate from IT for a variety of reasons, not least among them being the security of the grid.

The advent of smart meters, micro grids and the Internet of Things (IoT), coupled with the need to drive down costs to ratepayers, are forcing Utilities to begin consolidating their OT and IT infrastructures. This consolidation of systems is coming at a time when the volume and profile of cyber-attacks are increasing and the protection of Critical Infrastructure is under the spotlight.

As with most organizations, Utilities are facing a new reality. Maintaining the status quo as it pertains to cyber security is no longer a viable option. The Ontario Energy Board's creation of a new Cyber Security Framework in 2017 is forcing Ontario's LDCs and regulated entities to tackle cyber security as a business challenge. We understand that the Framework will be built, in part, against the National Institute of Standards and Technology (NIST) Security Guidelines. This will mandate increased efforts associated with proactive planning, rapid detection and timely response.

This Case Study concludes that:

1.) Existing in-house security resources and practices will not be sufficient to meet future requirements, especially for a more integrated IT and OT environments;

2.) Development of in-house expertise and tools will take significant time and be made more difficult as a direct result of the deficit of security expertise available in the marketplace. This approach would also drive up costs to ratepayers and shareholders by not leveraging shared tools, resources, expertise, and experience;

3.) Having developed Canada's first Security-as-a-Service (SECaaS), Stratejm is uniquely positioned to help Canadian Utilities close the security gap quickly and efficiently without requiring the need for major investments or commitments. Stratejm's SECaaS can be tailored to meet the evolving and rapidly changing external threat landscape.

Short and long term risks pertaining to cyber security for Utilities will be minimized through the incorporation of a Security-as-a-Service strategy. Stratejm can be leveraged to kick-start a rigorous security program that can enhance, augment, complement and supplement internal functions.

Contents

Introduction

Organizations are under intense pressure to defend against cyber-attacks and security breaches that can result in the theft of information, disruption of business continuity, reputational loss and the disabling of systems. Security is always an important business consideration, especially when public safety and consumer confidence are at stake. Regulators and shareholders alike are demanding that cyber security be taken very seriously.

In recent years Utilities have been the victims of an increasing number of targeted cyber-attacks launched by sophisticated adversaries. A security breach can have significant impact; possibly leading to loss of life or a major disruption in power quality, service delivery and reliability. This challenge is made more complex by the gradual convergence of IT/OT functions and the Internet of Things (IoT). Utilities must be aware of the unique threats and associated risks to their systems and be prepared to either accept or mitigate the various risks.

Specialized expertise, processes and tools are required for detecting and responding to disruptive events. Investing only in preventative technologies, which has long been the traditional approach, is no longer sufficient; best-in-class detection and response capabilities must now be supported as well.

A recent security pressure posture assessment conducted by Gartner concluded that Utilities have a **HIGH** security pressure posture. This means that the tolerance for risk is relatively **LOW** within the industry.

Understanding and effectively managing risk is most important when costs are a consideration. Utilities must strike a balance when considering the cost of security protection, the likelihood of an attack and the potential impact of an attack.

The risks associated with alternative options for implementing a security program can also vary – an in-house, do-it-yourself strategy is no longer a viable approach; it's too expensive and does not deliver on the best risk outcomes. Stratejm's Security-as-a-Service is proven to be a more cost-efficient and effective choice for Utilities of all shapes and sizes.

This Case Study highlights the advantages of service provision using Stratejm's subscription-based SECaaS and assesses the risks associated with specific security functions. It also looks at the challenges, risks and costs associated with building an in-house security program versus a pay-as-you-go subscription service as offered by Stratejm.

Potential Impact of a Cyber Security Breach

Any significant cyber security breach could lead to the following disruptive events, either separately or in combination:

1. Regulatory breach - i.e., violation of MFIPPA;
2. Financial loss - inability to bill customers if system data is compromised, fraud and/or fines;
3. Disruption of day-to-day business activity (loss of productivity and business continuity);
4. Reputational loss;

5. Disruption of the SCADA environment:
   a. Equipment damage to the grid;
   b. Power interruption leading to customer premise damage and lawsuits;
   c. Human harm – both employee and community safety (i.e. hospitals, traffic lights, nursing homes);
   d. Mechanical damage to customer-owned equipment; and
   e. Disruption of operations – i.e., working without the SCADA system;

Case Study Purpose & Scope

Our customer, a medium-sized Ontario LDC, had a requirement to ensure that their approach to cyber security minimizes the risks to systems and networks including IT and OT.

Our customer has limited resources who are dedicated to managing and executing the security function and did not have all the tools needed to implement security best practices. This includes tools for threat monitoring, breach detection, vulnerability management and response planning. These functions are critical components of the NIST Security Guidelines. The Case Study identifies and examines the major risks associated with **NOT** providing the following security services:

1. A Security Information and Event Management (SIEM) system for both the IT and OT environments;
2. Dedicated management for the SIEM system – i.e., having a system that is not fully supported and maintained and/or is not updated as the target systems evolve;
3. Ingestion of Threat Intelligence gathered and curated from the web, dark web and social media;
4. Vulnerability Management that incorporates internal and external scanning and is vertically integrated as part of an overall security program;
5. Proactive hunting for new emerging threats within the IT and the OT environments;
6. Expert staff and proactive processes for which the SIEM is a supporting tool; and
7. Appropriate vendor relationships to ensure optimal understanding of the evolving threat landscape.

Brief Service Description

The key security-related tools and services provided by Stratejm are:

1. IT Asset Management

IT asset management systems, which are oftentimes referred to as CMDBs or Configuration Management Databases, are more than just an inventory of physical equipment and contracts. The CMDB can keep track of a wide range of IT resources including equipment, systems, services, software, facilities and people as well as their inter-relationships. An IT asset management service should be used for both the IT and OT environments.

2. Log Management

A wide range of IT/OT-related activities, events and actions can be tracked using logging tools, and this data can be consolidated for analysis.

The examination of device logs is one of the primary methods for detecting security issues. In most cases, the logs are not reviewed in real time but are collected for off-line analysis and for correlating events across multiple devices. Logs can also be valuable for forensic investigations.

The log management system performs life cycle management of the log data. This includes the elimination of duplicates, detection of errors or missing data, and a variety of archival functions.

3. Vulnerability Management

Known vulnerabilities (i.e., the weak points in a system) are tracked and monitored

carefully by Stratejm. Plans will be developed to eliminate, avoid or mitigate all known vulnerabilities. Any changes in status will be recorded.

Common vulnerabilities include software patches not installed, old equipment with known security issues, data that is not backed up, hosted or shared systems and even devices that are not physically secure. Penetration tests (which are provided as a separate service) will usually find other less obvious vulnerabilities.

4. Threat Intelligence

Threat Intelligence, as defined by Gartner, is evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets.

Threat Intelligence can be used to inform decisions regarding the preferred response to that menace or hazard.

A variety of Threat Intelligence sources called "feeds" are available, such as from the federal government's Canadian Cyber Incident Response Centre. Stratejm works to access, filter and apply this knowledge to the benefit of our customers as part of an ongoing effort to enrich their security data warehouse.

The ability to render these services in-house are completely dependent on the availability of underlying resources including:

a. ***Security specialists*** to establish, maintain and operate the security services (including the associated processes and tools) and to plan the responses to known threats;
b. ***Asset management toolset*** to provide the CMDB functionality and to map the asset criticality to the potential threats to determine risk and identify changes;
c. ***Data management tools*** to supply data warehouse and business intelligence capabilities for consolidating, processing and analyzing all the data being ingested from the various sources; and
d. ***Threat intelligence feeds*** to collect external data from industry sources and to provide awareness and guidance concerning known and emerging security issues; this data can be filtered to create an early warning system for vulnerabilities and threats.

Our customer had very limited capabilities across the aforementioned resources.

Enterprise Risk

There exists real enterprise risk with not deploying the security functions described in the previous sections. Electing to maintain the status quo to protect against cyber-attacks was deemed unacceptable by the Board of Directors and Executive Leadership Team.

The four categories of risk that were identified and needed to be managed are listed in the box below:

Technical Risk – the likelihood that threats and vulnerabilities will exist undetected in a system or network;
Organizational Risk – the lack of people to perform essential tasks; a lack of appropppriate security expertise; and a low level of process maturity;
Operational Risk – the lack of appropriate procedures and tools; and
Contextual Risk – the impact of environmental issues, locational issues, brand and trust issues.

More specific risks for each of the security services are summarized in the following:

1. IT Asset Management

Issue: Due to the lack of support staff and tools available, IT and OT assets are not being tracked and managed very effectively - inventory control is manual; configuration relationships are not included; existing inventory data can be difficult to import into security tools.

Risks of not having sufficient IT asset information:

- Undocumented assets would be more likely to be lost or stolen;
- Device support and maintenance cannot be assured, leading to deployment vulnerabilities;
- System design changes can be more complicated and time-consuming;
- Assets may not be fixed and accessible (e.g., Cloud-based services, temporary systems);
- Financial and lifecycle control may be degraded or lost;
- Vendor management requires a detailed knowledge of installed assets;
- Asset knowledge informs vulnerability assessments and enables threat intelligence filtering.

Impact: Critical security functions will be unavailable or ineffective if assets are not tracked. Staff will be unable to implement even basic security practices if assets are not known.

2. Log Management

Issue: Due to a lack of technical expertise and defined processes, incident and change logs for applications and infrastructure are not produced, are not consolidated and filtered, and may not be monitored continuously. Incident detection depends on staff experience, their tenure with the company and due diligence.

If component state is not tracked and the relationships among components are not known, then there is no easy way to detect and respond to security events and incidents.

Risks of not managing log information:

- Logs may not be collected, consolidated or retained for a sufficient period;
- Log formats may not be compatible, may be inconsistent or may not be correlated;
- Incidents can remain undetected or their detection could be unacceptably delayed;
- Analysis tools may not be available, expertise to use the tools may be lacking or staff have no time to manage them;
- Historical records may not be properly maintained for forensic analyses;
- Vendor support for incident resolution would not be available without log files.

Impact: Even basic security management is difficult if records of activities and events are not maintained. Consolidation of data and matching it against system configurations is the basis for mitigating many risks; this is very hard to do after the fact.

3. Vulnerability Management

Issue: Every system has specific vulnerabilities at any given point in time. Expertise to identify vulnerabilities and mitigate the associated risks is needed. Without expert staff and the necessary tools, there is insufficient identification and tracking of vulnerabilities.

Knowing the status of assets (e.g. patch status) is also a requirement for establishing areas of vulnerability both for individual components and with systems.

Risks of not identifying and tracking vulnerabilities:

- Without a list of vulnerabilities, security staff will be unable to focus on known weaknesses;
- Efforts may not be directed at avoiding or mitigating existing or anticipated vulnerabilities;
- Pre-planning of attack responses will be more difficult and may be less targeted;
- Strong potential exists for attacks to go undetected.

Impact: Not knowing what vulnerabilities exist and what can happen if they are exploited makes it difficult to prioritize corrective projects and to be proactive in preventing incidents. Knowing the likely targets also enables proactive response planning and design.

4. **Threat Intelligence and Industry Collaboration**

   Issue: If the security experts have no time to maintain a level of industry awareness and to collaborate actively with peers, it will be difficult to collect, filter and make use of information that may be available from those who have already defended against an attack.

   Making use of threat intelligence is a specialized skill that requires expert staff to reach out and work with peers in other similar-type organizations.

   Risks of not participating in threat intelligence sharing:

   - Allocating resources to manage Threat Intelligence and participate in industry efforts can be expensive;
   - Threat intelligence serves as an early warning system for attacks, which would not be available if the services are not used;
   - Threat response planning can be more difficult if access to the experiences of others is not available.

   Impact: Available knowledge that could help minimize the impact of attacks or could identify vulnerabilities would not be available.

Risk Summary

Based on the services listed above, several major risks for LDC have been identified:

Major Risk #1: Existing staff will not be able to carry out all the activities necessary to achieve a high level of protection against compromises, intrusions or theft. This includes maintaining asset databases, researching vulnerabilities, participating in the threat intelligence community and continuous learning.

Major Risk #2: The ability to attract security professionals to build out the security function has been challenging and turnover was higher than expected due to a variety of external factors. Moreover, the Board of Directors is unwilling to invest in additional headcount as cyber security is not a core business function.

Major Risk #3: Security operations will consume most staff time, thereby reducing time available for planning and design of new systems, new tools and new processes. This will be especially risky if the use of cloud-based services expands and when IT and OT systems merge onto a common platform.

Major Risk #4: Funding for security may be weak and/or require frequent re-justification. Assuring a high level of protection must be a continuous activity, not a one-time project. Security support is becoming more complex as IT and OT integration develops.

It is noted that most of these risks are related to personnel and the staffing of security functions.

Developing security expertise and maintaining a security department is very difficult, costly and time consuming for management. Stratejm's Security-as-a-Services enables organizations to share the costs as to minimize the overhead and take advantage of the wider perspective available to external resources.

Cost Estimates

There are a variety of costs associated with establishing robust security practices, deploying security tools and building security expertise. The following estimates are purposely kept at a high level, but they do demonstrate the high cost benefit of Stratejm's SECaaS when compared to developing this function in-house.

Note: The costs identified on the next page are aligned with implementing the security functionality and solutioning required to effectively mitigate the risks identified within this Case Study. The cost estimates provided within both tables on the next page includes 24x7x365 monitoring and is based on a three (3) year term contract.

One-Time Charges (Capex)		
	In-House	**Stratejm SECaaS**
SIEM System	$175K	--
Implementation Services	$50K	$30K
Vulnerability Management	$25K	--
Hiring of Staff (6)	$96K*	--
TOTAL ($)	**$346,000**	**$30,000**

*Assumes that a recruitment or HR firm will be engaged to find prospective candidates. The industry standard reflects that the fee for service be equivalent to 20% of the base salary which we calculated at $80,000.00 per year.

Annual Recurring Charges (Opex)		
	In-House	**Stratejm SECaaS**
Staff Salaries/Benefits (6)	$660K**	--
Training/Education (6)	$60K	--
Threat Intelligence Subscriptions	$200K	--
Technology Support & Maintenance	$80K	--
SECaaS Subscription (Years 1, 2 and 3)*	--	$250K***
TOTAL ($)	**$1,000,000**	**$250,000**

*The supporting technology is updated by Stratejm as the service provider on an as required basis.

**We assumed a cost of $110,000.00 per year including immediate and deferred benefits for staff salaries. Six (6) staff is the minimum number required to support 24/7/365 monitoring.

***Includes IT and OT (SCADA) assets.

Recommendation

As noted earlier, our customer is a mid-sized Ontario LDC with a HIGH security pressure posture and a LOW tolerance for business risk.

The customer had two viable options for addressing the aforementioned risks and providing security services and support:

1.) Build a security practice in-house; or
2.) Outsource specific functions to a provider of managed Security-as-a-Service.

As evidenced by the data contained within the Cost Estimates section of this Case Study, the cost of Stratejm's SECaaS combined with the time-to-value when compared to building a comparable in-house security service is substantially lower. This benefits ratepayers, shareholders and stakeholders by providing best-in-class security at a minimal cost.

The services and functions outlined within this document are essential for the LDC to implement industry-accepted best practices and minimize its exposure to security incidents that can range from general embarrassment to major privacy breaches to full-scale service disruption. It is for these reasons that the customer elected to select Statejm as their trusted security partner.

About the Author

Don Sheppard P.Eng. is a Senior Consultant with ConCon Management Services of Toronto, Ontario. He has been a consultant and advisor for more than thirty-five years and participates in ISO standards development. Don is also an active blogger for IT World Canada.

About Stratejm Inc.

Stratejm has developed Canada's first Cloud-based Security-as-a-Service, enabling enterprise customers to solve security problems in a secure, intuitive and cost-effective manner. Time-to-value is optimized and the enterprise is under no obligation to purchase new hardware or software. Stratejm's security platform is backed

by a state-of-the-art Threat Intelligence Centre that is staffed by security professionals. Call 1-888-876-0504 or email to info@stratejm.com for further information.