Viewpoint paper

The secured utility of the 21st century

How utility industry trends are driving cybersecurity

Table of contents

Overview

In recent years, utilities have experienced a technology wave of digitization in their operational and IT environments. Every upgrade to generation, distribution, and field controls has brought a corresponding increase in risk. Likewise, risks to the utility enterprise increase as the IT environment races to support new customer interface portals, mobile applications, and integration with operational control systems.

This transition to digital-based systems, along with the new vulnerabilities they carry with them, has brought cybersecurity to the attention of utility boardrooms and governments alike. Consequently, utility executives are tasked to address these issues within an environment swirling with regulations.

This undertaking is made more difficult by legacy systems. They tend to be a mixture of rigidsystems, each operating within their own business silo with differing types and levels of security. The implementations and capabilities of legacy security systems vary widely, from those that provide application-specific security to those that provide database security to ones that provide integration adapters to enterprise security solutions. Some systems provide no security at all. As a result, this environment makes it extremely difficult to ensure the levels of security and customer privacy that regulators have mandated.

At HP we believe a different approach is required.

You need an architecture that instills cybersecurity across your enterprise, from your data center to your networks to your applications and at every endpoint. And you must accomplish all this while meeting strict governmental mandates, such as NERC-CIP. A haphazard approach or no approach at all leaves your utility at the mercy of punitive fines and costly attacks.

Fortunately, you don't have to face these challenges alone. Our security specialists have extensive experience developing best practices across many highly complex, business-continuity-critical, and well-regulated industries. They're well versed in helping utilities develop viable security strategies.

The HP approach rests upon a comprehensive security framework. It addresses your immediate operational security issues while setting your utility on the path toward developing a defense-in-depth security strategy.

Based on our experience, plus the insights of industry research analysts and organizations that we follow, we've identified five key trends impacting utility cybersecurity today. These are probably not new to you. Various research reports speak to them. They may use different wording to classify these trends or rank their importance differently, but by and large several major trends come into focus.

In our view, the top five trends that will drive the development and implementation of your utility security strategies are:

1. Security will become an enterprise-wide practice.
2. Smart grid scope is expanding to include distribution automation.
3. Data complexity and next-gen analytics will require an enterprise integration framework.
4. Demand for renewables will drive new distributed generation technologies and business models.
5. The consumerization of energy technology will carry new vulnerabilities to be addressed.

Strategic security considerations

What are the primary strategic cybersecurity issues facing utilities today? And what are the best ways for you to address them? Let's start at the beginning.

Historically, utility cybersecurity has been applied as a point solution to specific, siloed areas. For most utilities, that meant the implementation of discrete security solutions for generation, transmission, distribution, and IT systems. Typically, firewalls were created between each of these domains, each with their own resident security expert ready to declare them secure.

Unfortunately this approach results in veiled security, dubious accountability, and inconsistent monitoring policy management. Cracks can appear between the silos. And there is virtually no leveraging of security data, skills, and best practices at the enterprise level.

A comprehensive framework

Threats, along with the proliferation of potential entry points,[1] have rendered a siloed approach to cybersecurity obsolete. Thus utility security based on a patchwork of departmental or business unit solutions is too weak to counter current and emerging threats. Instead, we offer a long-term solution that takes a holistic approach toward cybersecurity. We subscribe to an end-to-end security framework applied across the utility enterprise (see Figure 1).

This approach recognizes the importance of cybersecurity and elevates it to the boardroom. In so doing, utility security becomes an enterprise-level function, complete with enterprise-level direction and accountability (e.g., board of directors, chief security officer, chief executive officer). By adopting this approach, your utility security becomes organic to your enterprise.

Our end-to-end architecture considers multiple layers within your enterprise, including governance, operations, the data center, networks, applications, and endpoint security. Existing processes such as identity management and virus detection will need to be addressed along with new processes such as data privacy and intrusion countermeasures.

Issues in data privacy and security

Why raise data privacy and security to the enterprise level? Due to the actions of privacy advocacy groups, public utility commission interveners, legislative bodies, and utility regulators, there are more data privacy and security requirements on utilities than ever before. These requirements and regulations come with punitive financial penalties executives can ill afford.

In this environment, an effective, enterprise-wide security architecture considers processes that safeguard data privacy and security. In the case of data privacy, for instance, it's necessary

Figure 1: Enterprise-wide end-to-end security framework

Security governance					
Assurance and auditing	Security risk management	System security certification management	Threat and vulnerability response management	Secure boardroom	Client security governance

Security operations						
Security operations	Threat intelligence	Security response	Security monitoring	Data protection	Digital investigation services	Identity and access management

Data center security	Network security	Application security	Endpoint security
Email security	DLP - in motion	DLP - in use	DLP - at rest
Database security	IDS/IPS	Web application FW	Enterprise mobile security
Web/URL filtering	Secure perimeter	Application vulnerability scanning	Endpoint protection
Cloud infrastructure security	Network access control	Secure application development and delivery	Encryption services

[1] See the discussion of digital devices in the operational security section.

to create new data-type groupings within the data taxonomy of your enterprise. These designations in turn help your applications, networks, and devices prevent the inappropriate sharing or disclosure of your customers' private data.

Another example of a data-type security issue is the handling of unstructured data in automated ways. Past utility security models rarely had to account for unstructured data types (e.g., Facebook posts, Twitter feeds, audio phone calls, video surveillance logs). Today, it's not possible to build a conprehensive end-to-end security architecture without addressing the vulnerabilities such unstructured data bring to the table.

An enterprise cybersecurity integration framework can help counter these threats while delivering much more value. For example, one of the benefits of a comprehensive security framework is the ability to assemble large data sets that may be mined for business intelligence. However, if handled improperly, data is vulnerable to unauthorized exposure through websites, emails, notification texts, or public portals. The consequences to your reputation, not to mention your bottom line, can be devastating. Thus your security architectures must be linked to your enterprise data architectures, which have been upgraded to handle unstructured data and promote the privacy of your data.

A secure data strategy considers information across its lifecycle

A comprehensive security architecture considers processes from beginning to end. This concept applies to your customer information as well, meaning that your data must be secured at every point in its lifecycle. The enterprise security architectures we've developed incorporate this lifecycle approach to data security. Moreover, our services teams (enterprise security protection, information management and analytics) use best practices based on the data lifecycle approach. We've also designed HP security software toolsets (ArcSight, Tipping Point, Fortify) and information management and analytics (Autonomy, Vertica) to support and reinforce this concept.

Architecture integration issues

Integration architectures, toolsets, and strategies require special attention. Many progressive utilities have encountered difficulties integrating the new generation of utility applications (e.g., CIS, CRM, GIS, DMS, OM) with legacy point-to-point technologies.

These utilities most often turn to service-oriented architecture (SOA) approaches in which they employ enterprise service bus (ESB) toolsets, agile development methodologies, and SOA governance. SOA tools and architectures can be powerful enforcers of enterprise security policy. Improperly used, however, they can leave data and processes unsecured. To successfully make the move, SOA approaches must incorporate adequate security design and testing.

A major driver for an end-to-end enterprise security architecture is granular visibility into essential operations. This includes the ability to provide complete operational monitoring, policy management, and compliance, as well as generate regulatory reports. Enabling this type of environment is critical for the cohesiveness of the overall architecture. We help you do this via a security portal. HP's Secure Boardroom is a robust portal capable of managing dynamic data inputs from heterogeneous sources; generating real-time alerts and updates to web, text, and mobile users; and supporting regular reporting for compliance.

Operational security considerations

Viewing utility operations through the lens of the five trends brings security vulnerabilities into sharp focus. As the industry evolves, we expect only to see them multiply, calling upon you to consistently hit a moving target.

And hit that target you must. Utility regulatory bodies (e.g., public utility commission, the Department of Energy, and North American Electric Reliability Corporation) expect you to have full, real-time enterprise-wide visibility into your operational security. This 24x7 operational awareness is critical to the efficiency and effectiveness of your operations. Viewed from a regulatory agency's perspective, your operational awareness is essential to maintaining a reliable grid – and thus foundational to the nation's safety and security.

So far we've established the need for a comprehensive cybersecurity framework to safeguard your operations and security. What does such a framework look like at the operational level? And how do the five trends affect these elements?

Distribution automation (DA) factors

The regulatory push for utilities to improve their conservation, efficiency, renewables, power quality, and reliability continues to drive most DA projects. Both DA and distribution management systems (DMS) represent a special class of monitoring and control systems because they are designed to ensure the reliability and efficacy of power delivery across the grid.

The architectures and software associated with DA/DMS have led to siloed security solutions. These have been augmented by the concept of "security through obscurity," the idea that if nobody knows about the architecture and software or is able to access them through modems or the Internet, the systems are thought to be safe.

In smart grid enterprises, DA/DMS become integral sources of time-sensitive, operational data that must be shared with other systems. In this way, DA/DMS can leverage device alarms, alerts, and power quality data available from smart grid meters and devices to more reliably deliver and optimize power to users.

Similarly, data from existing operational and business system applications (e.g., customer information systems, geographic information systems, digital metering, or demand response management systems) must be shared with DA/DMS. This integration enables a number of significant benefits, but it also exposes each system to security risks from and via the others.

Renewable energy system integration considerations

Further driving the need for operational integration is the growth of renewable generation sources such as wind, solar, and biomass. The concepts of distributed generation, virtual power plants, and microgrids all leverage the integration of DA/DMS with the utility to enable renewables.

This trend will gain strength in the coming years, as a host of social, environmental, and financial factors prevent new power plants from coming on line. Faced with rising energy costs along with the glaring inability of new plants to be built, individuals and businesses have started to field their own solutions.

Principally, their answer has been to deploy renewable wind and solar power-generating systems. As a result, utilities must be able to manage and control power flowing from distributed generation systems into the grid. That's no small feat, and it requires automation and intelligence.

For instance, customers' distributed-generation-control systems need to tie into your utility control system for you to access, monitor, manage, and integrate their power into your grid. However, doing so is a risky proposition because it provides a possible entry point for malware.

In addition to being a security threat, customer control systems have the potential to overwhelm your computer and network resources. Your control systems must have stable, predictable processing characteristics to properly function. Should a customer's control system malfunction, it could over-consume your network bandwidth, processing capacity, and/or available data volumes – leading to the denial of service to other customers' systems vying for the attention of your utility DA/DMS.

Your utility must protect against this malfunction-based denial of service as well as a malicious one. For example, a disgruntled customer may hold your utility liable for any equipment damage that they deem to be the result of a cyberattack that came through your utility infrastructure.

Large, complex volumes of data require robust business intelligence solutions to process them

The portfolio of new digital technologies coming to utilities continues to expand, bringing with it qualitative enhancements. For example, new technologies can upload data more frequently and at a much more granular level than utilities have experienced historically. Consequently, many utility companies are unprepared to handle the massive influx of data flooding their systems today.

As the number of smart meter and smart grid device deployments grow, so too will the security inputs flowing into the utility.

Take smart meters as an example. They're designed to transmit alerts in the event of tampering. An installed base of 500,000 smart meters experiencing even a one percent alert rate would yield 5,000 alerts. You could roll service trucks to check all 5,000 meters. However, we believe that a more effective solution is to correlate the alerts with information available elsewhere in your enterprise, be they work orders, meter history records, or firmware change records.

Smart meter alerts are but one example of many that your utility must consider. The prioritization of incoming data, along with its correlation with relevant sources to enhance security processes, will be a necessary enterprise-wide function. In this way you can minimize false alarms, prioritize real safety and security alarms, and better manage your grid resources.

Consumerization's effect on your business

Lastly, the consumerization of IT and the development of an "always-on" customer-utility relationship have dragged utilities into security and privacy areas they've previously not had to deal with. Long gone are the days where the utility-customer relationship was nurtured primarily with a monthly newsletter and an occasional call. Now, to be competitive, your company must incorporate new web, text, email, mobile-app, and anytime-anywhere service capabilities.

These tactics help you build closer relationships with your clients, engage them in your conservation and demand-management programs, and market new products and offerings to them. For their part, consumers want to take advantage of cost-saving and value-added programs and be better informed about service outages or other issues.

These changes present security challenges that must be overcome. For instance, your systems must authenticate and authorize users across your enterprise in a way that they can view only their data and execute only their authorized functions.

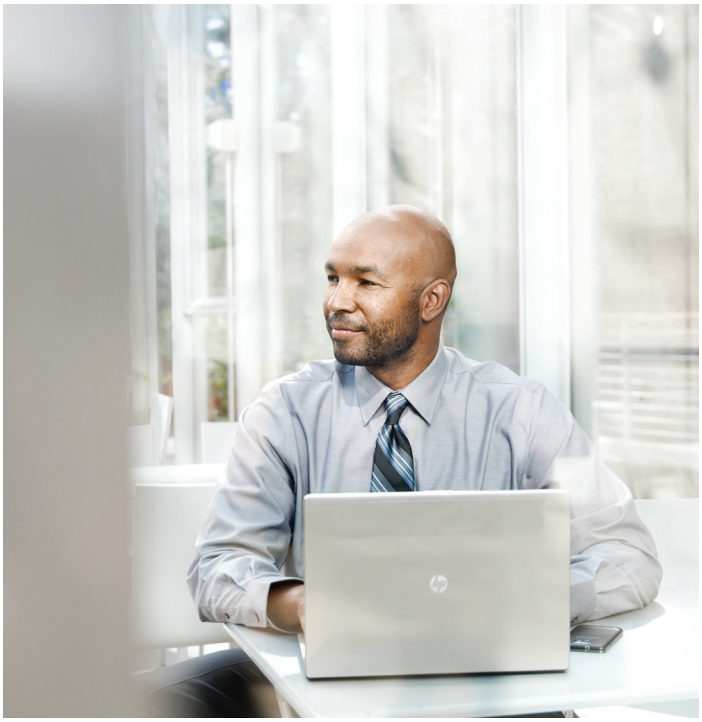
Add to that the need to comprehensively secure your customers' data across a wide range of consumer devices, via a multitude of channels, with 24x7 service availability.

HP knows cybersecurity and how to apply it to the utility industry

HP offers a complete security portfolio that's delivered by more than 3,000 dedicated security and privacy professionals. We have more than 40 years of experience delivering managed security services and have provided IT security consulting to leading businesses for more than two decades.

Capabilities

Our security offerings are based on the end-to-end enterprise-wide security framework illustrated in Figure 1. We offer comprehensive governance services to support your enterprise-wide cybersecurity objectives. Our end-to-end framework is comprehensive – not simply layered-on applications nor stuck-in firewalls. Moreover, our approach is designed to help your utility proactively adapt to evolving threats.



Our governance services include the integration and maintenance of your security policies and processes as well as their alignment with your business drivers, legal and regulatory requirements, and threat profile. These services focus on managing multiple suppliers and communicating the security and risk posture to your key stakeholders.

For example, the HP Secure Boardroom gives you granular visibility into your security operations from the strategic level down to the tactical incident and security performance level.

HP's security operations services

The HP security operations services support your security functions and processes. With HP, you have two options. You can choose to contract our managed services to run your security operations, or you can outsource this security function entirely to us.

To support both options, we built five state-of-the art Global Security Operations Centers equipped with redundant systems and top-of-the-line security infrastructure and applications. These include HP's ArcSight application, which collects data from across your enterprise and:

- Gives you granular visibility into your security operations
- Simplifies your compliance reporting
- Detects advanced and insider threats

Whichever business model best fits your needs, our end-to-end cybersecurity incorporates the capabilities of our risk management software suite and managed security services.

Security consulting, managed services, and technology services

Each of these service groups may be applied to better secure four key areas in your enterprise: your data center(s), networks, applications, and endpoints.

HP data center security services: Our data center security services are designed to help you effectively secure your email and database systems. They provide comprehensive web/URL filter solutions as well as intensive cloud infrastructure security offerings.

HP network security services: To help you secure your network layer, HP offers services to manage data in motion, firewalls, and network access controls. We also leverage the capabilities of the HP TippingPoint appliance, which protects physical, virtual, cloud, and hybrid environments through application-level content and context awareness. Combined with research through DVLabs, it provides vulnerability analysis and discovery, ensuring that you have the best preemptive protection for vulnerabilities and zero day issues.

HP application security services: Successful security at the application security layer rests on the protection of information in use. This includes securing point-applications as well as leveraging web application firewalls.

We offer powerful tools to help you achieve these ends including HP Fortify Software Security Center, a suite of tightly integrated solutions engineered to fix and prevent security vulnerabilities in your applications. It integrates application security testing through onsite or as-a-service models for advanced testing of commercial, custom, and open-source applications.

HP Fortify eliminates your software security risk by ensuring that all of your business software is trustworthy and in compliance with your internal and external security mandates. And by "all" we mean multiple platform types and your in-house software applications as well as those you procured from third parties.

HP endpoint security services: The trends in this paper point to the rapid and ubiquitous increase in the number of endpoint vulnerabilities that you will need to guard against. For these, we offer a comprehensive suite of services in the areas of DLP-at rest, enterprise mobile security, endpoint protection, and encryption services.

And while we bring the full force of HP capabilities to bear in these areas, we realize that your environment is unique and requires services and solutions that enhance your experience. Therefore, we leverage the capabilities of our global Agility and Technology Alliance partnerships to deliver services from some of the world's leading IT security service providers, including McAfee, Symantec, and Check Point to name a few.

Conclusions

As digitization continues to proliferate across your enterprise, security vulnerabilities will increase accordingly. Smart grid, renewable energy, and consumerization trends alone will incorporate vast numbers of new endpoints to be secured. Alarmed by the growing potential to disrupt power supplies, governments and regulatory bodies are acting. Thus, utility executives must grapple with reams of new mandates and reporting requirements to secure their systems.

Because some of your most dangerous antagonists are well organized, your response to them must be calculated. Based on our experience, along with the major trends we see shaping the utility industry, we believe that the most cost-effective, long-term pathway to meeting these challenges is to adopt an enterprise-wide cybersecurity architecture.

Not only does such an approach meet regulatory guidelines such as NERC-CIP, but it also positions your enterprise to systematically overcome vulnerabilities and threats. It exploits your information to develop actionable intelligence upon which you can quickly act.

The road ahead is complex with many potential pitfalls. HP can help you sidestep those pitfalls, as well as develop and implement a comprehensive strategy to secure your utility.

Cybersecurity is not new to HP. We've successfully delivered cybersecurity consulting services and products to the finance, military, and government industries for many years. We've developed proven best practices and amassed centuries of collective experience among our enterprise security employees. And we've applied that knowledge to develop utility-specific tools, processes, and methodologies that can build an enterprise security strategy for your future.

When you work with HP, you gain a partner that is dedicated to helping you secure your enterprise. In this way, we free you to focus on running and growing your business.

To learn more about how HP can help your utility strengthen its cybersecurity, visit us **www.hp.com/go/utilities**.

Get connected

hp.com/go/getconnected

Get the insider view on tech trends, support alerts, and HP solutions.

Share with colleagues

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA4-3292ENW, Created August 2012