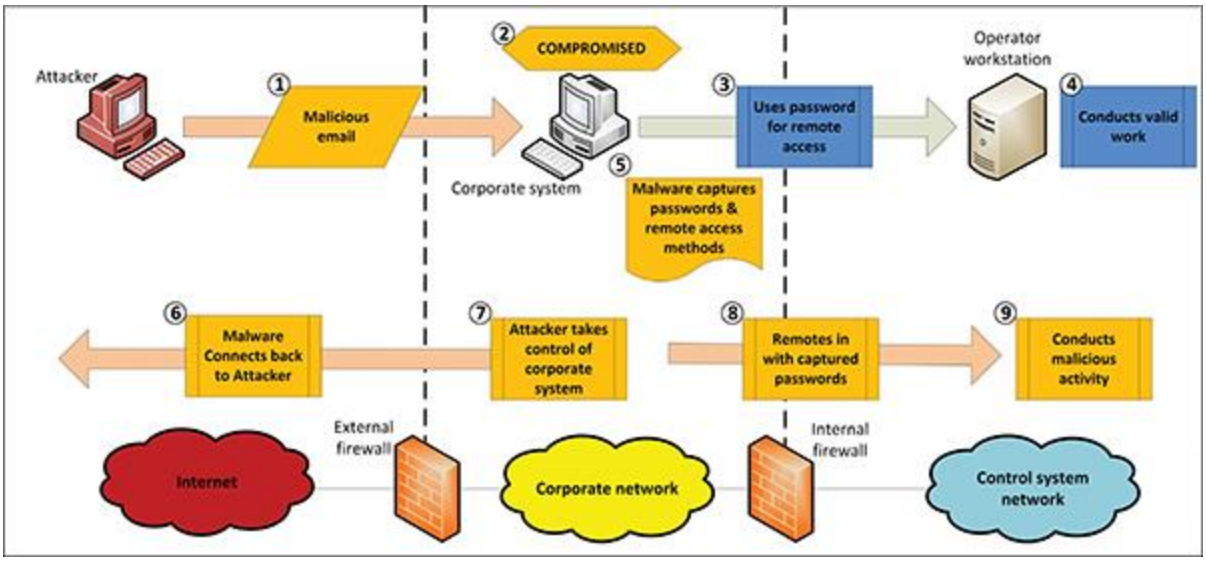
by Eamonn McCormick, Scott Marshall & Gustav Hoyer

Integrating security into the IT/Business architecture is a vital aspect of modern enterprise architecture and solution architecture. Utilicast specializes in the energy industry and there is a particular focus on security as it relates not only to IT but to Operations Technology (OT) as well. Indeed, at Utilicast we believe that security is an overriding concern that impacts all aspects of the energy business. We also believe that it should be the number one architectural concern in the energy industry followed by proper strategic alignment of IT. Critical mission capabilities (reliable service etc..) and rapidly changing business drivers are a big demand. In short maintaining security while maintaining reliable cost-effective service and responding to strategic business drivers is an overriding concern in the energy industry.

The reason we feel security is so important is that energy underpins the health of our society and economy. Energy companies play a vital role in the economy. Disruption to the energy system as witnessed in Puerto Rico causes chaos. Natural disasters are still the biggest threat to energy supply to date. Perhaps the biggest threat to energy system disruption in the future is not actually natural disasters but "cyber war" scale attacks on our energy infrastructure.

There is growing evidence that "cyber war" is a clear and present danger to the energy industry. For example the December 2015 Ukraine power grid cyberattack took place on 23 December 2015 and is considered to be the first known successful cyberattack on a power grid. Hackers could successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers. Most affected were consumers of «Prykarpattyaoblenergo» (Ukrainian: Прикарпаттяобленерго; servicing Ivano-Frankivsk Oblast): 30 substations were switched off, and about 230 thousand people were left without electricity for a period from 1 to 6 hours.[1]



Ukraine Attack

The potential of malevolent state or non-state actors to effectively wage cyber warfare against countries by targeting energy infrastructure is a huge threat that energy companies must take very seriously. The ability of state and non-state actors to attack our core institutions (think election interference in 2016) and the growing cyber warfare capabilities of adversaries like North Korea means the threat to the energy industry is growing.

Indeed, one could argue that including security architecture in the core DNA of architecture is now vital. We can no longer security function "bolted on" to business and IT. Security must now be integrated into all aspects of the company DNA. Security is not just a "techie" thing it impacts all aspects of architecture from motivation, business process, applications services, PAAS (Platform As A Service) and IAAS (Infrastructure As A Service). In addition, we need to integrate security into the core IT delivery services like operations and support as well. Our observations are that the energy industry is working hard on cyber security issue. It has the attention of the "C-suite". There have been tremendous improvements made and executives and employees are typically committed to success. There is also a strong sense of urgency. However, we also see that our customers and other players in the industry continue to struggle with the security challenge. Despite best efforts progress is often slow. Why is that?

What we have observed is that security is often difficult to integrate into the architecture of a company because the existing architecture was largely developed without security as a "top of mind" concern. As a result, the architecture typically has significant vulnerabilities "from the get go" so to speak. Because the architecture has pre-existing "security holes" it tends to be addressed "piecemeal" rather than as a

systemic challenge. This makes implementing security solutions more difficult because it becomes a "patching what already exists" issue versus a "we need to rethink things ground up from a security perspective". Even new projects tend to be "bolt ons" from a security perspective because they are integrating into an already "weak" security foundation. The fact of the matter is that security impacts all aspects of the architecture. Most architectures evolved without a coherent security approach. Therefore, patching the existing "security holes" in the existing architecture becomes the defector "only available" approach. A patching mentality while well-meaning results in the reality that there is seldom a coherent strategy in play to integrate security. Rather the "patch" mentality is born of the exigencies of the moment and the well-meaning employees get swamped with trying to patch what already exists, versus stepping back and perhaps solving the problem in simpler and more complete ways. The security threats we are now facing continue to evolve. "Patching" is a losing game where we see companies constantly remediating point areas of weaknesses. This is often hard work and conducted with the best intentions. However, this can never deliver true security unfortunately. Security can only truly come from a more integrated approach. Therefore, because security is an ever-changing discipline we must admit that the patch approach can no longer succeed. Ultimately the patch strategy cannot keep up with an ever-evolving cyber threat and is doomed it to failure. Even more troubling as we now move into the era of "cyber warfare" some of our most precious energy infrastructure may be vulnerable to a catastrophic and coordinated attack.

One of the unfortunate things we have observed in the security industry is that it tends to encourage lots of specialization and a lack of clarity on how to approach security more systematically. The industry tends to "peddle products" in a way that solves only partial aspects of real world problems. We have seen many excellent point solutions from vendors in organizations who understand critical aspects of security, but they struggle to make an impact because there is no way to systematically weave what they should offer into the DNA of the organization itself. We also often lack a complete view of how we are implementing security holistically and how to focus our resources most effectively to reduce risk at an acceptable cost. So how can we evolve from piecemeal approach to something more holistic? We certainly don't lack for security frameworks like NIST but our ability to systematically implement complex frameworks is questionable at best. It is just too complex. This is not aided by the fact the technologies to support security often overlap, are often fragmented and are not clearly differentiated from each other. Technology vendors do not help by selling ambiguous product offerings that often only cover a small aspect of the security landscape.

Our Utilicast approach on how architects can address this is to align the company on a simpler set of core security architecture principles. By simplifying the problem and boiling it down to a simpler "human understandable" set of principles we can embark on a pragmatic approach to implementing those principles across the organization. The basic idea is that "if we can apply a simple set of principles consistently across the architecture" we are better off that focusing on implementing the hugely complex frameworks. However, we see principles being mapped back to frameworks, however the goal of the principles is to cover the "vital ground" in a simpler more holistic way. So, what is a principle?

What is A Principle?

A principle represents a qualitative statement of intent that should be met by the architecture.

Principles are strongly related to goals and requirements. Like requirements, principles define intended properties of systems. However, in contrast to requirements, principles are broader in scope and more abstract than requirements. A principle defines a general property that applies to any system in a certain context. A requirement defines a property that applies to a specific system as described by an architecture.

Security Architecture Some Initial Principles

Defining a set of security principles that meet your company's needs can take time. The following are a few key principles that may be useful in getting you started.

Principles should be designed to align with the core security processes of identify assets to protect, protect those assets, detect security events impacting those assets, respond to those events and recover from the security event and remediate the root cause or implement counter measures where possible. Using this simple process driven approach to security is very "human understandable" and works well.

An initial principle is that security is an overriding enterprise architectural concern that must be aligned with business risk management. Security is somewhat like insurance. How much is the business willing to invest to mitigate security risk. Recently security has become the dominant nonfunctional requirement for the typical energy enterprise. Therefore, improving security posture should be identified as a critical element of any program involving modernization of IT and business processes. The degree the business invests in security however is a function of enterprise risk management. Security cannot easily be implemented after the fact" so it has to be

built as part of the DNA of critical systems and the enterprise architecture as a whole. Good security is not cheap and a and the business must decide how much it wishes to invest to mitigate the risk. It is hardly fair to blame IT for security breaches if IT has inadequate resources. Likewise, business cannot be blamed if IT is not realistic about what it will truly take to secure the enterprise. A decision needs to be made on an ongoing basis how much investment is needed to manage the security risk - from a business perspective. This architecture and business driven risk approach is a core principle and elevates security concerns to a business concern primarily.

At Utilicast we have identified 30 other key principles which need to be tuned to the needs of individual customers. Below are a few more principles for example you may want to consider.

One key idea underlying modern security principles is the concept of the "tenant" based security. A tenant is a group of users who share a common access with specific privileges to a certain collection of software services. Th trend in the industry is to segment applications in groups of related applications typically an eco-system linked to a core application like the energy management system, metering system of customer billing system. Establishing a logical set of application domains that map to tenants is a key premise of cloud based architecture.

Another important security principle is "Private like public"– this can be summarized as companies should adopt best security tenant practices from cloud leaders like Amazon and Microsoft. Microsofts's basic premise is that tenants should not trust each other or lower security assets. For example, tenants should not trust other tenant app ecosystems, workstations, the "general" internal network or other tenants. Part of the rationale for this principle is that it allows the organization to more easily adopt the latest security architectures and make them their own. The other rationale is that the hybrid model is now the defacto reality for almost all organizations. A large percentage of apps are heading to the cloud so it only makes sense to organize as if everything were cloud based so you can maximize security, portability, availability as well as security. The days of the "flat" internal network are over.

Zone based threat defense. Zone based threat defense implies security in depth. By defining zones of security, we can differentiate between levels of trust - for example the simplest is untrusted, semi trusted, trusted and restricted. Getting clear on security zones and mapping tenants to zones is a critical starting point. While the zone based defense concept is not new, it is not often implemented. Combining the zone defense and tenant concepts can simplify how this will be implemented.

Linking of security, applications domains and tenants to the concept of infrastructure as a service. The tenant idea must be related to a infrastructure as service set of services that implement the tenant security policies. Exactly what this means can vary but there must be an infrastructure pattern that support the security policies that you wish to implement at the tenant level.

Now that we have the basic idea of tenant and its relationship to applications and infrastructure understood we can return to the higher-level principles such as:

Aligning application domains to IAAS tenants, to business capabilities automatically aligns security to business capabilities. Security can then be aligned with business risk management more easily – security investment becomes a business risk decision directly related to IT assets associated with that business unit. This simplifies investment decision making and drives accountability.

Security services are configured to the needs of tenants based on business risk decisions (investment driven by business risk assessment). Security becomes a "business unit" top line quality metric.

Cloud Access Security Broker Services are required given how important SAAS/PAAS is to the modern enterprise. Having 10 different ways to connect to the cloud is untenable and fundamentally insecure. A CASB is needed to protect the company from cloud threats and should take "cloud to cloud" interactions into consideration.

In a security architecture engagement, we review these types of concepts with IT and business. We work with business and IT to translate them into a defined set of 20 to 30 security principles that make sense for that enterprise. We then link the principles to company security and compliance control sets so we ensure the principles cover the bulk of the security controls pertinent to the company. Then we look at how best to implement the principles. For example, we may look at how the application tenants needs to be mapped to security zones. We then move on to what needs to be done to provision specific technology services and related service offerings to enable the principles.

The threat of cyber terrorism to the energy industry is real. We at Utilicast are successfully applying the principles based approach at several leading energy companies. Please feel free to contact Scott, Gustav or I if you wish to know more.

Thanks for your time.

ghoyer@utilicast.com
smarshall@utilicast.com
emccormick@utilicast.com