Sofaer International Case Competition 2015

The Cyber Age – From Virtual Hazard to Reality

The Cyber Age – From Virtual Hazard to Reality

The Cyber Age – Not Only a Virtual Hazard

In June of 2009 in the midst of the Iranian national election and the political turmoil that led to the forceful submission of opposition, thousands of Iranian computers started to crash. Perhaps initially perceived as a government attempt to control information and social networks, this was in fact just one of the symptoms of the world's first cyber weapon. Cyber- attacks had certainly been recorded much earlier, but the Stuxnet computer worm that hit Iranian nuclear infrastructure facilities, and later also devastated peripheral civilian devices, was a precedent in the importance of its target and the severity of the damage it caused. Originally physically inserted into the system, allegedly using USB devices, to infiltrate and interfere with Iran's Natanz uranium enrichment facility, Stuxnet caused centrifuges to over-heat and crash at a rate that neither local operators nor international inspectors were able to explain. Only in June of 2010, more than a year after the first malfunctions began to appear, did a security company from Belarus discover that a spore of files apparently causing crashes on Iranian PCs were somehow linked to the infrastructure of the Iranian nuclear plan.

As early as 1998, US President Bill Clinton pointed out that cyber and physical threats to US infrastructure have the potential to damage critical bloodlines of the American nation, placing specific emphasis on the cyber threats. As always, Hollywood saw it first, showing hackers patch into physical infrastructure using cyber methods for financial incentives in the 1992 cult film Sneakers.

Today, experts claim we are in the midst of a full blown cyber war; even if we can still very comfortably and allegedly safely surf the web through countless mobile and stationary devices,

Udi Aharoni from the Eli Hurvitz Institute of Strategic Management at the TAU School of Management, Tel Aviv University, prepared this case with the assistance of Alon Epstein, Erez Cohn, and Shira Lifshiz as the basis for a case competition. The case does not intend to illustrate effective or ineffective handling of business processes or decisions.

everywhere, and at any time – but this is exactly what makes the cyber threat so devastatingly dangerous.

Despite the sensational media coverage, the cyber-attacks on Sony Pictures and Home Depot, in which credit card information was stolen from the companies' information technology (IT) systems are only minor incidents. The threats to virtual networks and information databases are nothing to be trifled with, but perhaps pale in comparison to hacking physical infrastructure, which has the potential to threaten our way of life. A notable recent example documented hackers who gained access to the production network of a steel mill in Germany in December 2014 and then prevented a blast furnace from being properly shut down, causing massive damage. Also, earlier that year, the US Department of Homeland Security announced it would investigate the possibility that the Havex Trojan had targeted industrial control systems compromising over 1,000 energy companies across Europe and North America.

Incapacitating a power plant, or even just a substation, might cause massive blackouts, leaving hundreds of thousands or even millions in the dark for weeks on end. Hospitals have emergency generators, but after 24-48 hours their fuel supplies will be depleted, leaving critically ill patients without respirators, operating rooms without lighting. Deprived of energy, 21st century medicine will be pushed back into the Middle-Ages. The threats are not only to power supplies. Water purification and distribution systems are under constant threat, as are oil and gas lines, and mass transportation systems are in danger of being compromised. The global shift from analogue to digital systems opened up endless prospects, but it also signaled the coming of the age of cyber wars.

The most recent suspected attack occurred in Turkey on 31 March 2015, when two major power plants defaulted, diminishing the general grid's capacity by roughly 10%, and leaving more than 80 million people in the dark. Every part of Little Asia from the Greek border in Eastern Europe to the very edges of the Iranian frontier had experienced blackouts.

All recent events demonstrate that cyber warfare has two spearheads, one that is completely virtual, threatening zettabytes of data that the human race has accumulated; the other is capable of causing destruction in the physical world.

C.H.E.W. Global Cyber Threats

Devising a comprehensive and effective strategy to defend critical infrastructure from cyber threats would require governments and businesses to understand the threats themselves, and who would be potentially behind them. In November 2014, Admiral Mike Rogers, commander of the U.S. Cyber Command, witnessed before the congressional Permanent Select Committee on Intelligence that foreign nations are capable of attacking US aviation infrastructure, energy plants, transportation networks and financial companies. This statement came just following the discovery of the Russian "BlackEnergy" Trojan inside software responsible for running critical US infrastructure; these malicious computer worms could be used to stage large-scale attacks. Earlier in 2014, the FBI released information on "Ugly Gorilla", an attacker that invaded the control systems of utilities in the United States. In what was suspected to be a scouting mission, Ugly Gorilla gained the cyber keys necessary for access to systems that regulate the flow of natural gas.

Are these government organized attacks, or rogue individuals with a personal agenda? Richard Clarke, a former special advisor on cybersecurity during the Bush administration, coined the C.H.E.W. acronym, defining the four different motives for cyber attacks:

Cybercrime: The notion that someone is going to attack you with the primary motive being financial gain from the endeavor.

Hacktivism: The motive of attacking someone based upon a difference in ideologies. The primary focus of these attacks is not financial but rather to persuade or dissuade certain actions or "voices."

Espionage: The straight forward motive to gain information on another organization in pursuit of leverage (e.g. political, financial, capitalistic, market share, etc.).

War (Cyber): The notion of a nation-state or transnational threat trying to tear down the centers of power of an adversary via a cyber attack. The attack could be on non-military targets like critical infrastructure or financial services, or more traditional targets such as the military industrial complex.

Attacks arising from such motives can be carried out by governments, organized entities, rogue organizations, violent digital dissidents, or any of these in combination, such as governments employing bodies to camouflage strategic attacks and covert interests. Be that as it may, detecting and preventing these attacks has become a strategic challenge, and requires a multi-disciplined approach – first and foremost a technological one.

Command & Control of Critical Infrastructure – Applying a Security Perspective

Infrastructures are complex networks of physical and software assets. The physical assets are electrical, mechanical, hydraulic, and additional types of equipment. These are monitored by sensors and controlled by legacy systems that allow users to interface with them and regulate their use. These complex infrastructural systems are managed by a supervisory control and data acquisition (SCADA) system, or an industrial control system (ICS). SCADA/ICS systems are connected to a human-machine interface (HMI), enabling controllers to oversee the relevant processes, detect any changes, and perform necessary adjustments.

Infrastructure networks have two distinct technological environments that often interact with each other. The physical environment is connected by operational technology (OT), while management and business processes are performed by an information technology (IT) system. All organizations utilize IT systems to facilitate decision making, communication and internal/external processes. These are perceived as vulnerable because of their connectivity with the outside world and are of course commonly protected by security measures. OT systems, on the other hand, are seldom protected by cybersecurity means, for various reasons that are no longer relevant. OT systems are often closed circuit systems, connected to an internal independent SCADA server. However, it is an illusion that infrastructural networks are truly closed, and perhaps this very perception is what makes them vulnerable to cyber threats.

Power utility networks comprise substations in which power is generated, regulated, distributed, and stored. These substations are widely dispersed over vast geographical areas, in order to provide end users with a constant, reliable, and safe supply of energy. If a substation is hacked through physical means, malicious software can be sent throughout the entire grid. In

other words, the immediate threat is the compromising of the targeted substation, but the bigger threat is the potential to bring down the entire grid from a single point of access.

The grid can also be accessed centrally; workstations, which are connected to the central SCADA server, can be tampered with, thus sending viruses and hazardous worms throughout the entire network. In 2007, the Department of Homeland Security of the US government designed an experiment now known as Project Aurora that involved hacking into a replica of an Idaho power plant's control system and causing it to smoke, shake and self-destruct. The experiment proved that these allegedly closed networks can be hacked and physically damaged using cyber agents. The Stuxnet worm that hit the Iranian nuclear plant in 2009 was inserted through USB devices used in the central control station of the Natanz plant.

Another point of entry to the OT system is through its interface with the company's IT system. Decision support systems require interaction points and information flow between OT and IT. These interaction points are supervised and firewalled, but they still constitute a weak link and potential point of entry to hack into the OT, thus compromising physical assets. In the attack against the German steel mill in 2014, the attackers gained access through the plant's business network using a spear-phishing email, working their way into production networks to access systems controlling plant equipment.

Points of entry to the closed OT system are apparent to both hackers and operators alike, but often these are not safeguarded to the extent that IT systems are.

Radiflow – Securing Infrastructure

In this melee of hackers vs. security, quite a few technologies and companies are competing on a global pie of thousands of infrastructures. The service providers, be they power utilities, water purification and distribution companies, or oil and gas rigs and pipelines, wish to operate in the smoothest and most efficient manner. Downtimes entail immense losses, with every hour that systems are offline (substation, turbine, relay unit, pump unit, pipe blockage, etc.) estimated to cost approximately $20,000 to $500,000. Though this is an extremely broad range, even at its conservative end it promises an almost unbearable financial burden, damage to assets and a

possible threat of casualties. Thus, providers are inclined to take certain measures to prevent potential disasters.

This is where Radiflow comes in. Established in 2009 by Ilan Barda and Rafi Horev, employing 25 engineers, mainly cybersecurity experts, software programmers and industrial automation experts, Radiflow is privately owned by the RAD group, one of Israel's leading ICT consortiums, founded by Zohar and Yehuda Zisapel in 1981. As part of the RAD group, Radiflow utilizes the group's supporting services such as manufacturing, finance, and HR. This arrangement enables Radiflow as a start-up to focus its efforts on the technology challenges and to minimize its expenses during its growth phase.

Radiflow was one of the first companies to identify the cybersecurity risk evolving in the critical infrastructure of modern installations and was founded on the basis of an innovative idea on how to address this challenge. Radiflow provides cybersecurity to client companies, using a cutting edge solution that combines hardware and software to detect and prevent attempts to hack into their critical systems. Radiflow designed an appliance that can be integrated in remote substation units, providing local security, network regulation, and prevention capabilities. The remote units are connected to a central intrusion detection system (IDS) that performs unique anomaly detection algorithms designed by Radiflow and interfaces with the client company's SCADA servers. Once an intrusion is detected, the central system alerts the remote substation units to isolate themselves and shut down if necessary. This prevents any malicious attempts to bring down the entire system. Moreover, the remote units control access to the system, and when necessary can prevent even authorized personnel from reaching parts within the network to which they normally have access. This not only defends against malware infiltrating the systems, but also against negligence and improper use of the system.

Picture a scenario in which a rogue terrorist unit wishes to bring down an entire city's power grid. In order to do so they devise a plan to break into an isolated substation at the edge of town, hack into the OT system through one of its service ports, and implant malware that will cause cooling turbines to work at a mere 10% below standard speed. A supervisor sitting at the command & control center will see an indication that a certain cooling turbine at the edge of town has diminished capabilities, but nothing dramatic, and will perhaps even dispatch a service team. The controller is ignorant of the odds that the tampering will spread to the entire grid in

just a few hours, causing all cooling to gradually drop, threatening to overload the entire network, and even decommissioning units for long periods of time. Had the controller realized that the physical manifestation was an indication of a cyber attack, he would have been able to isolate the substation and further investigate the event. Using Radiflow's system, companies are able to receive indications that a cyber attack has occurred, identify the location of entry to the system, and isolate the threat before any damage occurs.

How Companies and Executives Regard Security Threats

Israel is considered one of the leading economies when it comes to cybersecurity, a fact due not only to its advanced technological capabilities, but also to necessity. Israel, its government institutions, private sector companies, and infrastructure assets are under constant cyber attacks. In 2014, the Israel Electric Corporation (IEC) identified 47,000 malicious programs in its system, compared to several hundred just the year before. This enormous increase tells only part of the story; these droves of nasty codes were responsible for approximately 183,000 to 293,000 cyber-attack attempts a month on IEC systems. The company's chairman was quoted saying that around 865,000 attempts were documented during a single summer day in 2014. The IEC is an extreme example, but perhaps utility and infrastructure companies throughout the globe should be looking at IEC as a benchmark for what they can expect in the years to come.

Back in 1998, President Bill Clinton issued the following statement: "I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems". Since then many regulatory motions have attempted to promote cyber protection of critical infrastructure, the most significant being that issued in April of 2014 by the US Federal Energy Regulatory Commission (FERC). Version 5 of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) set new standards and guidelines on cybersecurity of critical facilities of power utilities. Since then, the number of requests for security assessments has increased, but the baseline is so low, that the market has still not scratched its potential. In a survey conducted by Black & Veatch in 2014, half of the participants – executives from utility and critical infrastructure companies, responded that they did not have

integrated security systems, though a greater percentage of the investor-owned utilities did have such systems. Only one year before that cybersecurity was identified as an area of concentration for major investments by only 1.7% of respondents. This evidence certainly indicates that awareness and promotion of cybersecurity is rising, but the extremely low starting position and slow pace, are not encouraging for security providers.

When no company or home PC is without a firewall and active up-to-date antivirus protection, how is it that critical infrastructures are left vulnerable to cyber attacks? These are just a few of the answers:

- A false feeling of security – since the OT network of the utility is separate from the IT network it is assumed that it is secure, and the threat of an insider attacking the OT network is still not acknowledged.
- The complex legacy OT systems – adding cybersecurity systems to already unique and extremely complex systems is very challenging, and requires many adaptations of the security systems and the OT controlling software.
- The conservative culture of infrastructure companies and their professional staff makes them slow decision makers, reluctant to change traditional processes. Moreover, they often remain oblivious to the severity of the threat, until it is too late. In addition, nearly 50% of respondents in a Black & Veatch survey conducted in 2014 believed that physical asset attacks would either stay the same or decrease. Considering the overwhelming evidence, this notion seems to be wishful thinking.
- Regulation up to now has called for reliability, rather than mandating physical security protection and compliance; such regulations have just been put into place. Regulation protocols set standards and are essential for sound corporate governance, but at the same time compliance is predictable, which might make it the hacker's best friend.
- Cybersecurity measures will have to be placed throughout the grid, forcing revisions on central and substation units, and entailing extensive training of service staff members, who are usually not IT experts and thus lack the required basic understanding of such new technologies.
- The cybersecurity solutions are not always cheap, and despite the fact that infrastructure and utility companies are not short on funds, they are reluctant to spend

large amounts to prevent potential threats, that just might skip their company. At the end of the day, it's like insurance: you buy it so you won't have to use it. If you don't know what might hit you, if at all, and what damage it might cause, then why buy it in the first place?

What even further complicates the issue of cybersecurity for utility and infrastructure companies is the question of who calls the shots? These companies are usually large, complex bureaucratic systems that have been around for decades, honing elaborate procedures for making these sorts of decisions. Thus, even if IT and security professionals within the companies are strong advocates of cyber resilience, the actual decision might lie elsewhere in the organization – in operations, engineering, controlling units, for instance. Organizational decision making is always a challenge, but with the prospect of radical changes that need to be put in place, forcing widespread and massive compliance and adaptation in the company, opposition comes easily.

May 2014 was a turning point for many executives and stakeholders from all sectors, when the president and CEO of Target, the US's third largest retailer, was sent packing following an information breach of the company's IT system that caused the cyber theft of sensitive customer information. Had this happened to a critical infrastructure company on which millions rely to sustain their way of life, things might have been catastrophic. The fact that boards of directors and executives are liable and expected to pay a personal price for these sorts of events indicates a change in mindsets. Considering that cyber attackers are numerous and persistent – for every one identified there are a hundred that were not, recent developments should sound alarms amid executives and companies that provide critical services and among the people responsible for protecting citizens from attacks.

Segmenting Infrastructure

In the Black & Veatch 2014 strategic directions analysis of the US electric industry, it is stated that in 2009 the industry estimates called for an expenditure of over $50 billion on cyber assets, with 15-18 billion for utilities. This astronomic figure might not be unreasonable, but evidence shows that companies simply are not spending anything that can come close to this estimate. In their market report, IHS noted that in 2013 the market size of industrial cybersecurity (a broader

market than just critical infrastructure, including the automotive, machinery, food & beverage, pharmaceuticals, and other non–relevant sectors) stood at approximately $600 million, and was projected to climb to $1.2 billion by 2019 at a compound annual average growth rate of 12%. The critical infrastructure portion in this growth estimate and certainly of market value is the most significant, estimated to be around $168-$251 million (based on different sources), a very long way from Black & Veatch's multi-billion dollar estimates.

The security market consists of three types of competitors:

- Vendors that provide both IT and OT security such as CheckPoint and PaloAlto.
- Automation companies that also provide security solutions, such as GE, ABB, and Siemens.
- Exclusive OT infrastructure security solution providers similar to Radiflow

Out of the components of the critical infrastructure market, power generation, transmission, and distribution are the largest, followed by oil and gas, and water utilities.

Electricity and power

The largest and most regulated sector for SCADA/ICS security solutions (and threats) is automated power grids, with an estimated value of around $251 million for security outlays alone. This sector should be analyzed through two distinct perspectives – that of the providers and that of the integrators. The providers are those corporations that own the infrastructure and are responsible for the entire value chain of production, transmission, and distribution. These are the utility power companies, geographically dispersed and charged to deliver reliable energy to all their customers.

On the other side of the coin are the integrators, or automation companies that provide turn-key solutions for the providers in some or all elements of the value chain. These are usually global giants selling their products and services to providers worldwide. Corporations such as Siemens, GE, Mitsubishi, Alstom and others, manufacture critical grid elements, and also provide continuous services to maintain and upgrade them. Since these corporations often manufacture and service the electricity providers' SCADA/ICS systems, they are also in charge of designing their security capabilities, protecting critical systems from outside hacking. Many if not all of the integrators have basic security capabilities, embedding their own or their partner

company's engines within the automation controllers and the SCADA servers to detect cyber threats. However, most lack advanced security capabilities that can detect the sophisticated attacks occurring within the network.

Specializing companies like Radiflow on the other hand have developed advanced capabilities not only to detect interventions, but also to prevent them on the central and substation levels. While their capabilities are indisputable, it is extremely difficult to persuade integrators and utility companies to install these complex systems.

Apart from their high cost, another reason for the reluctance to use advanced security systems such as those provided by Radiflow is the fact that part of the capabilities they provide is restricting technicians' access to the entire system, granting them passage only to limited parts. From the perspective of the utilities and system integrators, restricting their technicians' access to substations and central elements of the grid to accommodate the requirements of the security system may limit the efficiency of remote maintenance operations, so it is not necessarily in their best interest. From the perspective of the security provider, without limited access, any technician is capable of bringing down the entire system intentionally or by mistake. Moreover, technicians can gather sensitive information on any part of the system just by accessing it from a remote site, under the pretense of servicing a substation turbine.

Oil and Gas

The second sector in terms of size is security for oil and gas, from extraction on rigs, refinement, distribution and conversion. This sector's size is estimated to be around $94.3 million, including refinement and the petrochemical sectors. Like power grids, oil and gas infrastructures can be accessed centrally from a command & control unit, but also somewhere along the way through endless kilometers of pipelines. A malfunction in any part of the process can not only cause losses of billions of dollars' worth of substance but also pollution that will still be around for our grandchildren's children to bear. With their fewer access points and less complex distribution networks, oil and gas lines might not be as vulnerable as power grids, but they run in extremely remote locations throughout vast geographies, making them difficult to physically protect and easier to tamper with.

Water

Another critical feature of modern civilization is water. As for the previous critical assets, pumping, filtering and distribution of water are vulnerable to hacking attempts. Any failure within the system has the potential to leave millions of people without this most basic living substance. In many countries water systems are extremely complex, relying on desalination, sewage refinement, deep water extraction and other means to sustain population needs. All these processes are digitally reliant, and therefore vulnerable to malicious cyber attacks. The market value of ensuring security in the water sector is estimated to be around $44.6 million.

Products and Security Capabilities

Applying a simplistic dichotomous approach, cybersecurity of infrastructure can be divided into basic solutions, usually integrative to the SCADA/ICS of the operators. On the other hand, the advanced solutions require deeper changes to the systems, involving additional hardware and software, and training of relevant personnel; these solutions however provide comprehensive defense and prevention capabilities.

As always in complex sales, relationships are everything. The threats and destructive potential of a cyber attack on critical infrastructure are not overlooked by the infrastructure operators and the integrators. Introducing an advanced solution into such an emerging market starts with informative meetings to arouse awareness amongst potential clients regarding the threats and the advantages of the proposed solution, followed by a gratis pilot test. Radiflow performs an initial survey to learn the basic features and normal behavior patterns of the client's SCADA server, after which they are able to detect any intrusion that exceeds the system's normal parameters.

Once the pilot has proven effective, decisions need to be made on whether or not to purchase the full system. Revenues from a single sale could vary anywhere from $100K to $1M; regardless of cost, decisions of this nature are often very slow. If an affirmative decision is finally made, Radiflow completes the survey to establish an accurate baseline of the client's SCADA system, studying its patterns, communication interfaces and many other parameters critical to the

process. Radiflow hardware is connected to substations throughout the grid, or pipeline, giving peripheral indications as well as central awareness of any hacking attempt.

Most cybersecurity companies working with critical infrastructure have an advanced intrusion detection system (IDS), but what distinguishes Radiflow is the fact that they have also developed an inline intrusion prevention system (IPS), capable of providing active defense capabilities that will cut off and isolate any potentially malicious code inserted into the system. Operation of the system is handed over to the owners, after the hardware and software have been successfully integrated and company operators have been trained to interact with the new security protocols.

Essentially, Radiflow sells a turn-key solution, but as software generations advance and the technology becomes more sophisticated, the company also offers a product & service package, granting system upgrades, and additional value added services to clients. To date, sales are limited to just over $2 million annually, posing great challenges for the company.

Marketing efforts mainly amount to conferences, newsletters, investing in relations with leading integrators and US labs, which in turn recommend considering Radiflow solutions to decision makers.

The Future of Radiflow

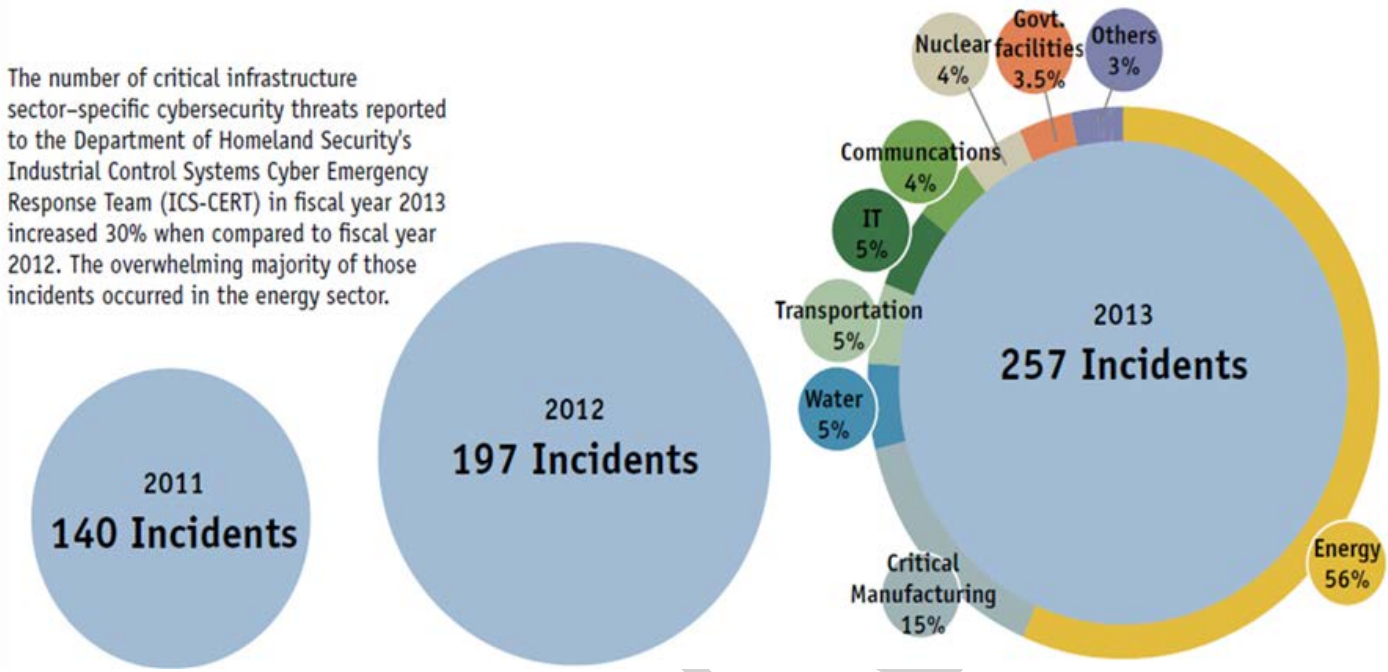
In order to position itself as a leading force, Radiflow will first have to assess the realistic materialization rate of the market and decide how aggressive it should plan its go-to-market efforts.

Once this is decided, Radiflow should analyze and weigh the different sectors and geographical markets, the various direct and indirect competitors in each segment, and accordingly explore and choose its strategic opportunities along the industry value chain.

The company must adopt a strategic solution that in the next few years will take it from a small Israeli start-up company, to a prominent global player with significant revenue growth. Any strategic solution should take into account the resources required to obtain the set goals and desired capabilities, the chances of obtaining them, and the risks associated along the chosen path.

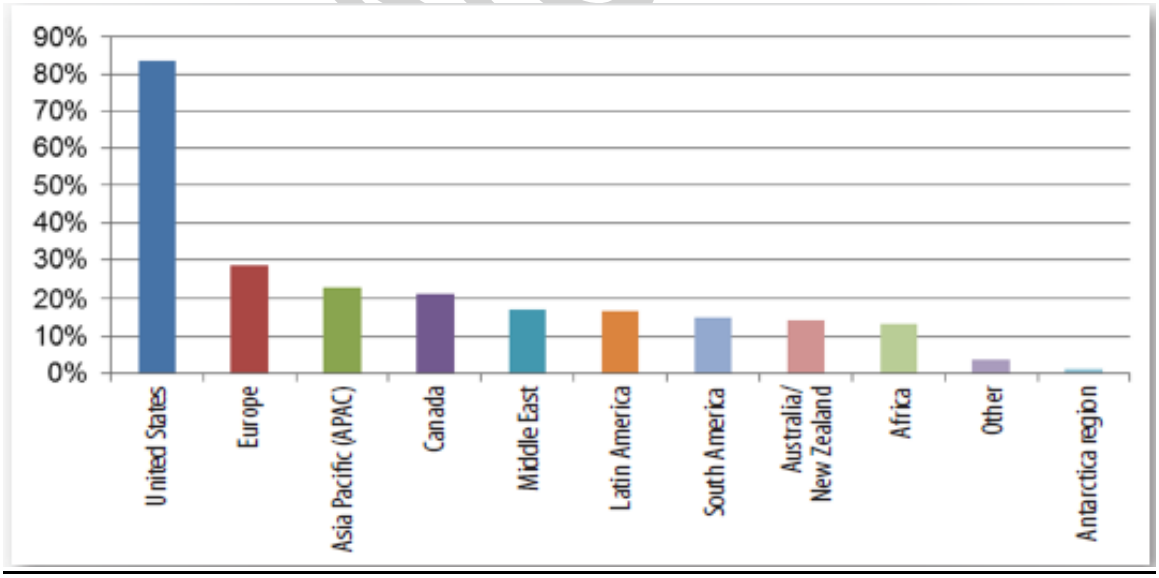
Appendixes

Exhibit 1: Reported Cybersecurity Threats in 2013



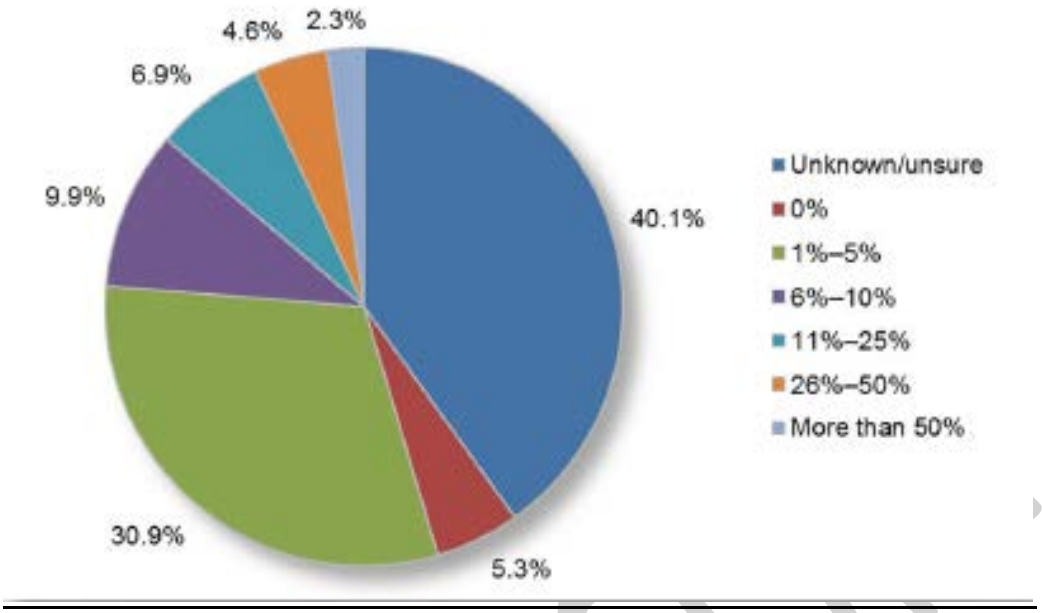
Source: ICS-CERT — copy and artwork by POWER magazine, March 2014

Exhibit 2: Worldwide Allocation of Control System Operations



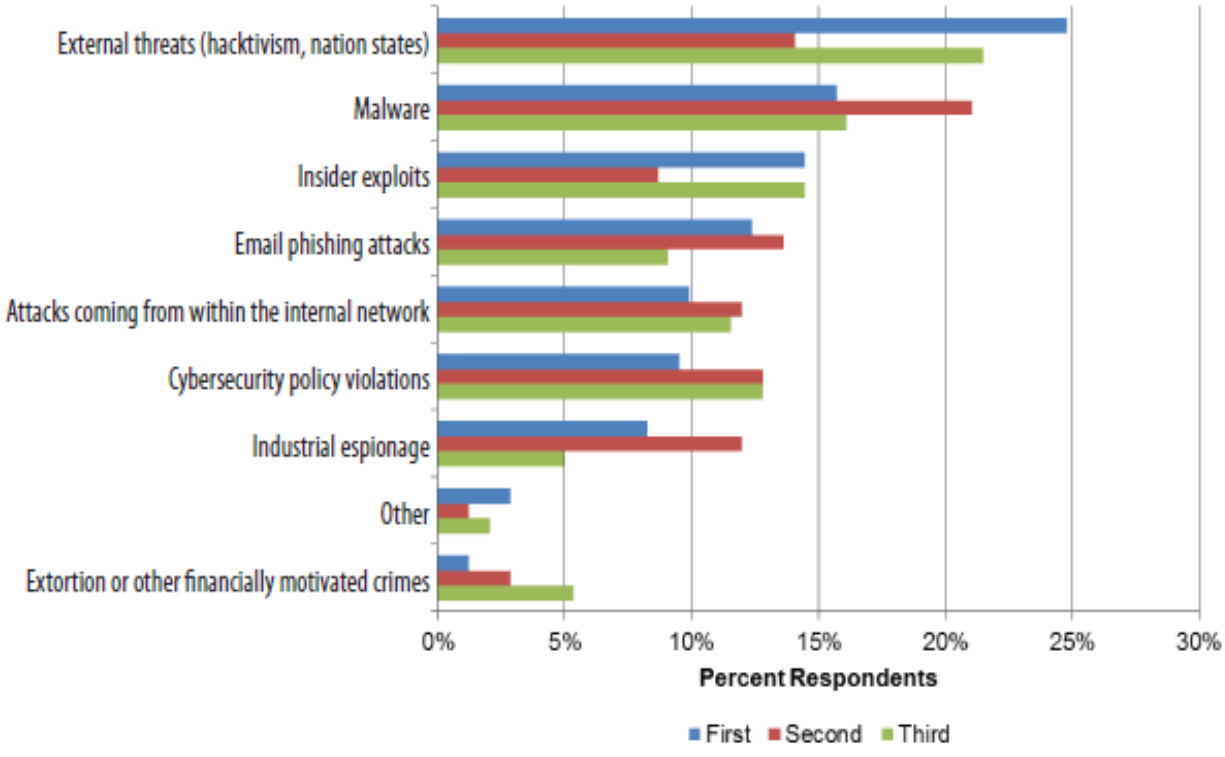
Source: SANS™ Institute, Analyst Survey, 2014

Exhibit 3: Cybersecurity Budget Allocation



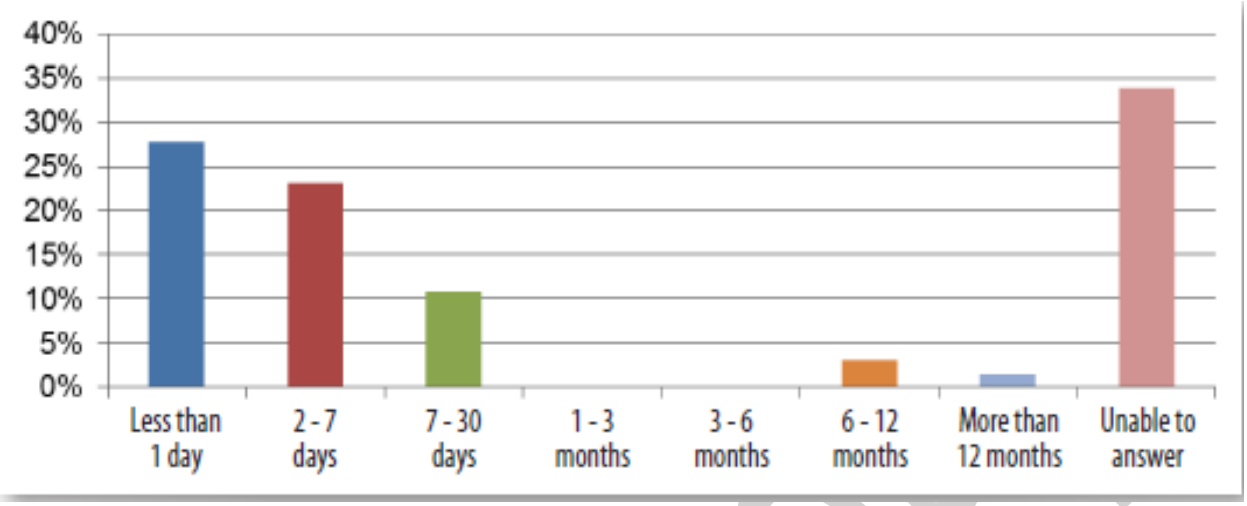
Source: SANS™ Institute, Analyst Survey, 2014

Exhibit 4: Top Threat Vectors



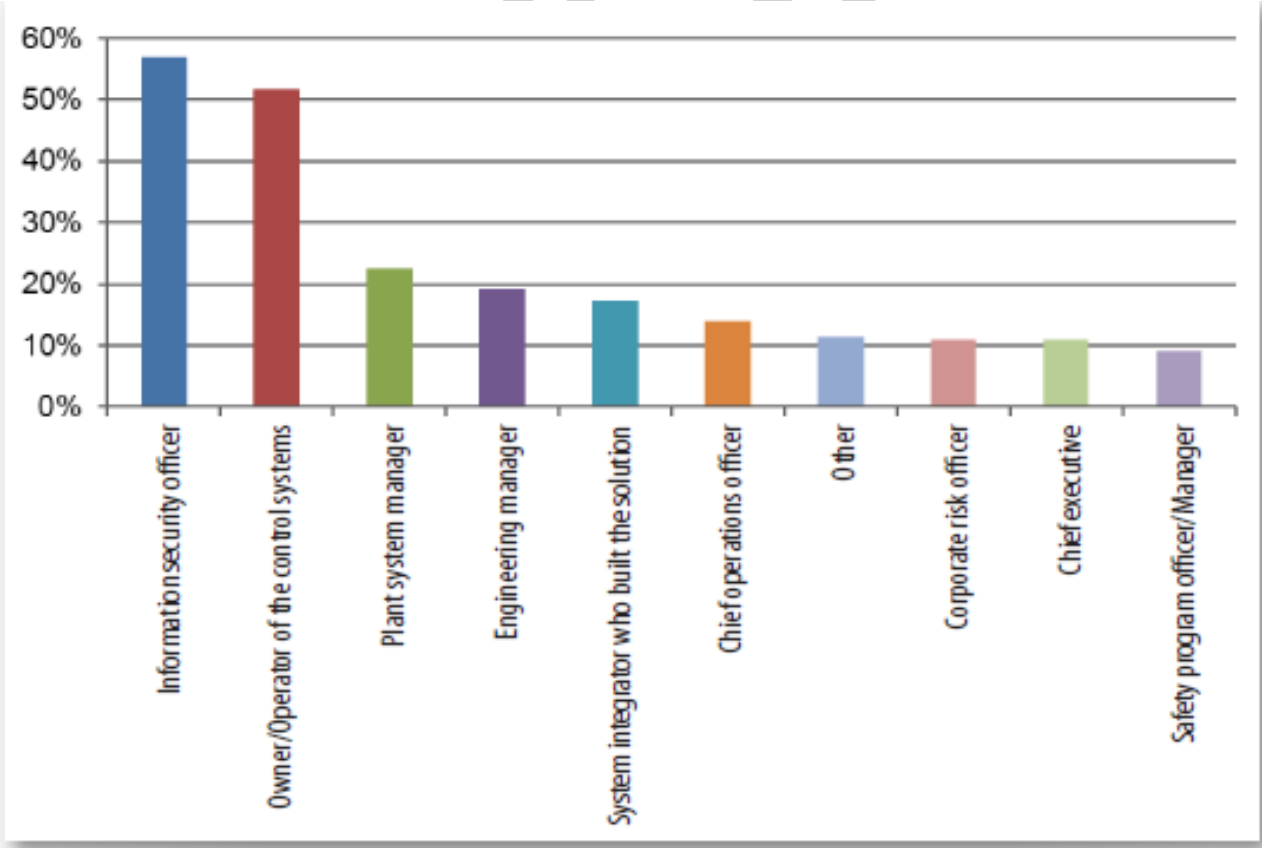
Source: SANS™ Institute, Analyst Survey, 2014

Exhibit 5: Exposure to Detection Time Period



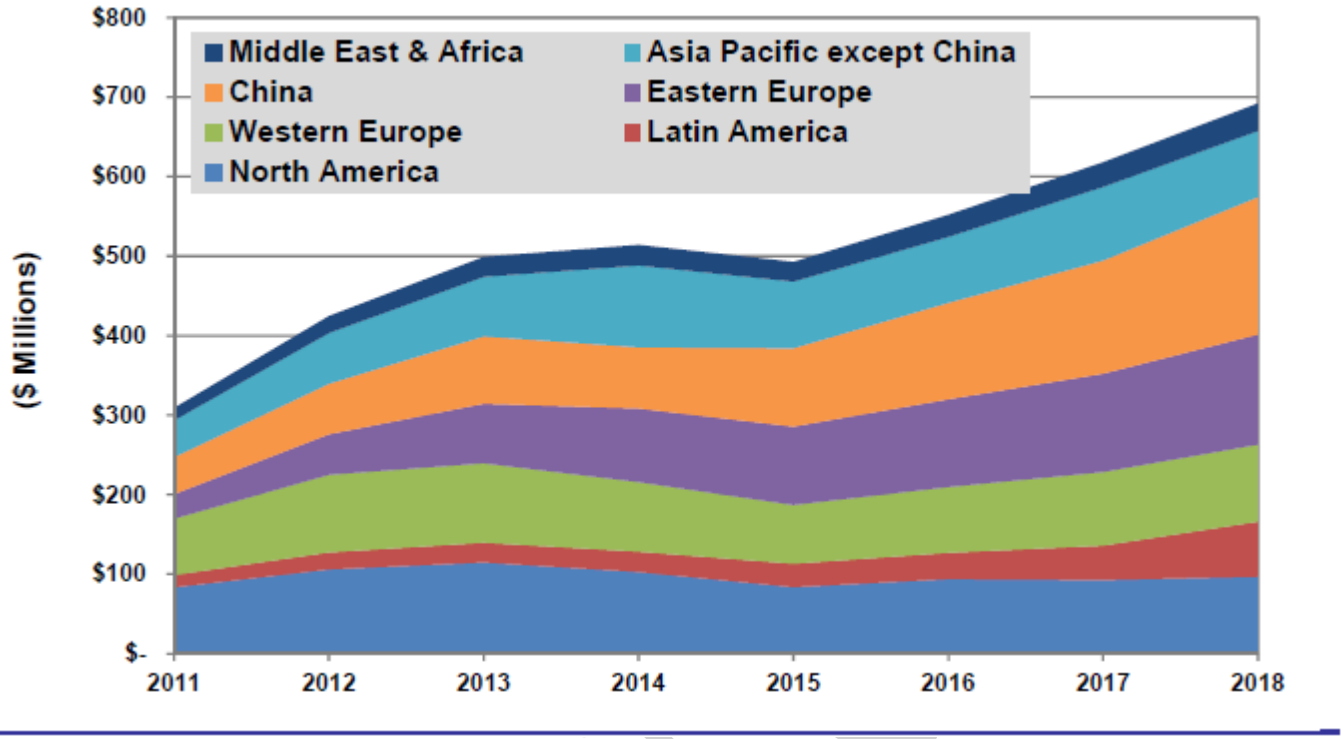
Source: SANS™ Institute, Analyst Survey, 2014

Exhibit 6: Responsibility for Security of Control Systems



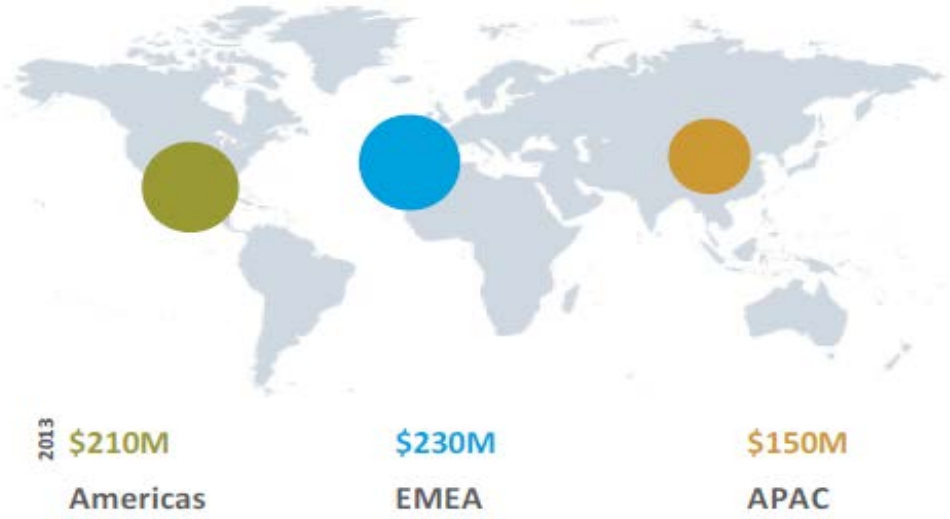
Source: SANS™ Institute, Analyst Survey, 2014 ??manager with a small m on the far right

Exhibit 7: ICS Security Revenue by Region, World Markets: 2011-2018



Source: Pike Research, 2011

Exhibit 8: World Market by Region



Source: Market Report - Cybersecurity in Process and Discrete Automation, IHS Technology, 2014

Exhibit 9: World Market for Industrial Cybersecurity Products by Industry, Revenues (Nominal 2013 dollars, in millions)

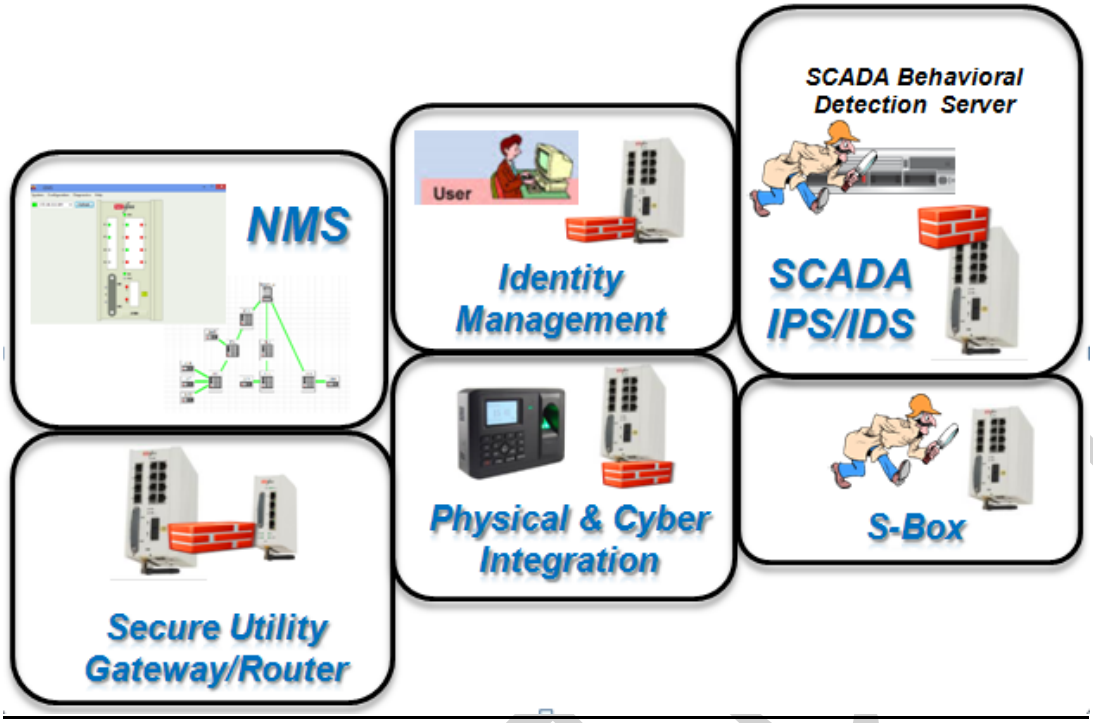
	2013	2013-2019 Trendline	CAGR 13-19
Automotive			
Revenues ($M)	4.4		6.2%
Machinery			
Revenues ($M)	59.2		19.5%
Other Discrete			
Revenues ($M)	5.4		5.8%
Chemical			
Revenues ($M)	62.6		9.9%
Food and Beverage			
Revenues ($M)	10.6		8.9%
Oil and Gas			
Revenues ($M)	83.5		8.5%
Refining and Petrochemical			
Revenues ($M)	10.8		8.4%
Pharmaceuticals			
Revenues ($M)	6.1		8.3%
Power Generation			
Revenues ($M)	109.7		12.1%
Power Transmission and Distribution			
Revenues ($M)	141.2		15.6%
Water/Wastewater			
Revenues ($M)	44.6		10.6%
Other Process Industry			
Revenues ($M)	51.0		9.2%

Source: Market Report – Cybersecurity in Process and Discrete Automation, IHS Technology, 2014

Exhibit 10: Remote Unit

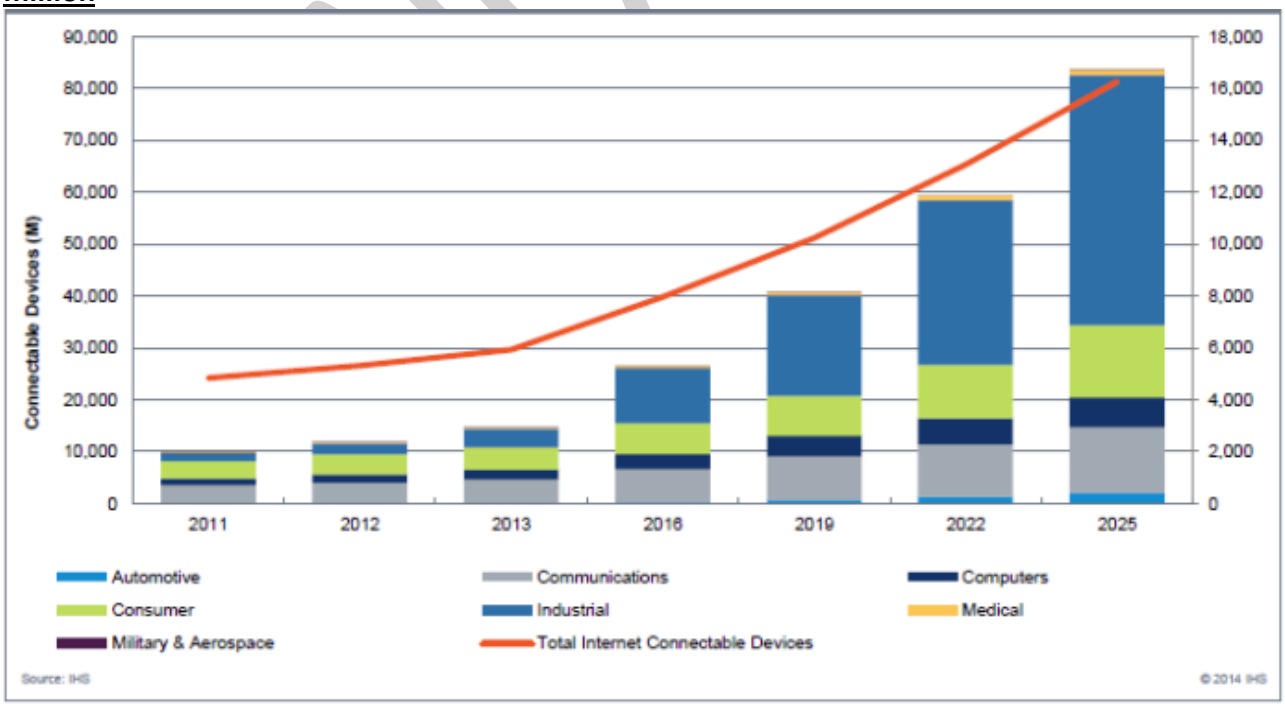
Source: Company data

Exhibit 11: Radiflow Portfolio Evolution



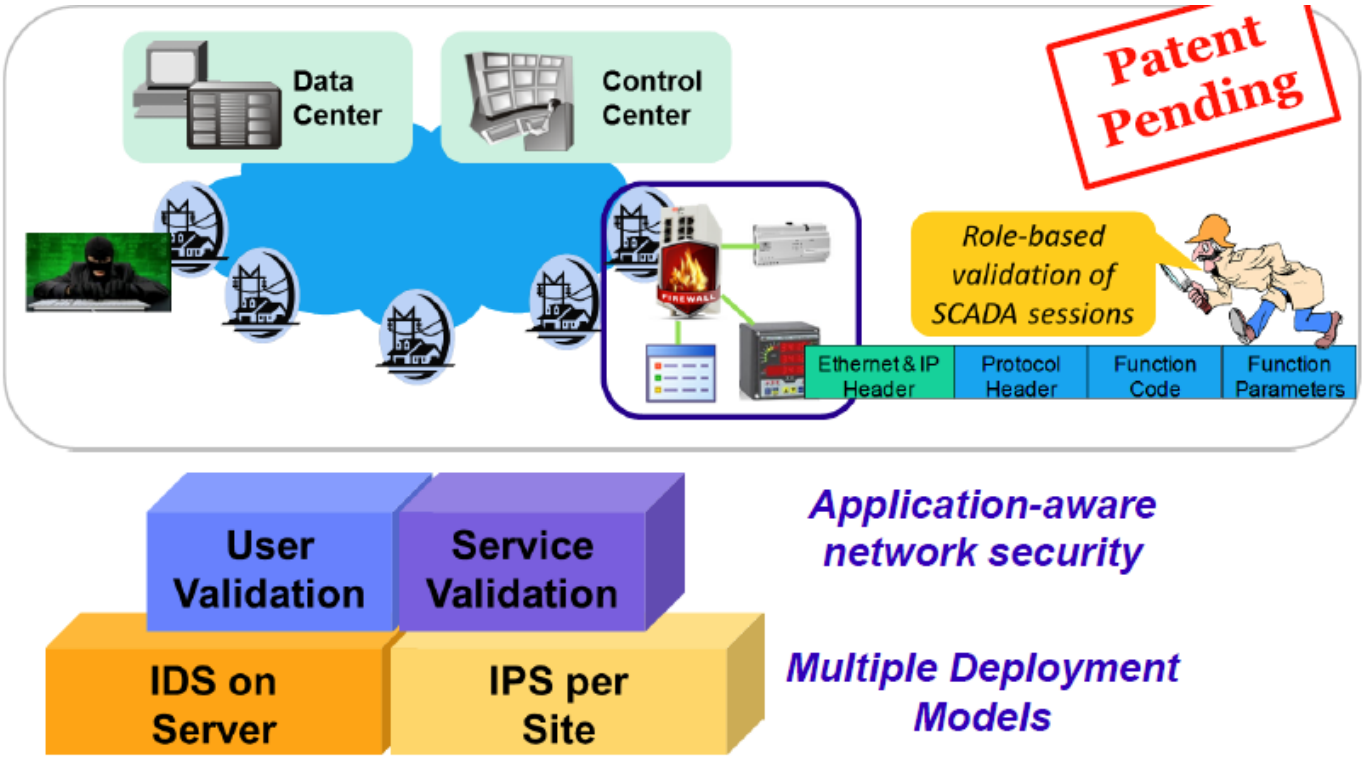
Source: Company data

Exhibit 12: Internet Connectable Devices – Installed Base & New Shipments 2011-2025, $US million



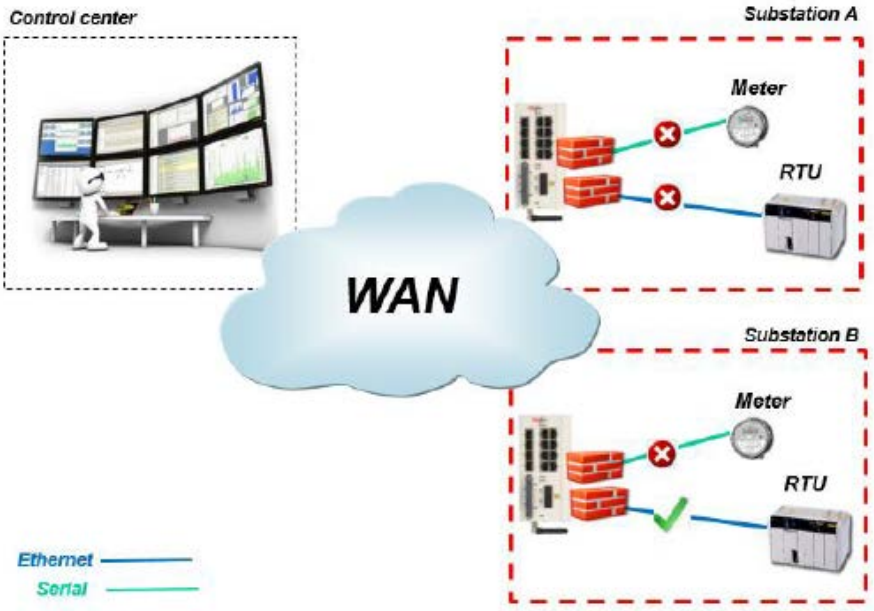
Source: Company data

Exhibit 13: Radiflow Solution



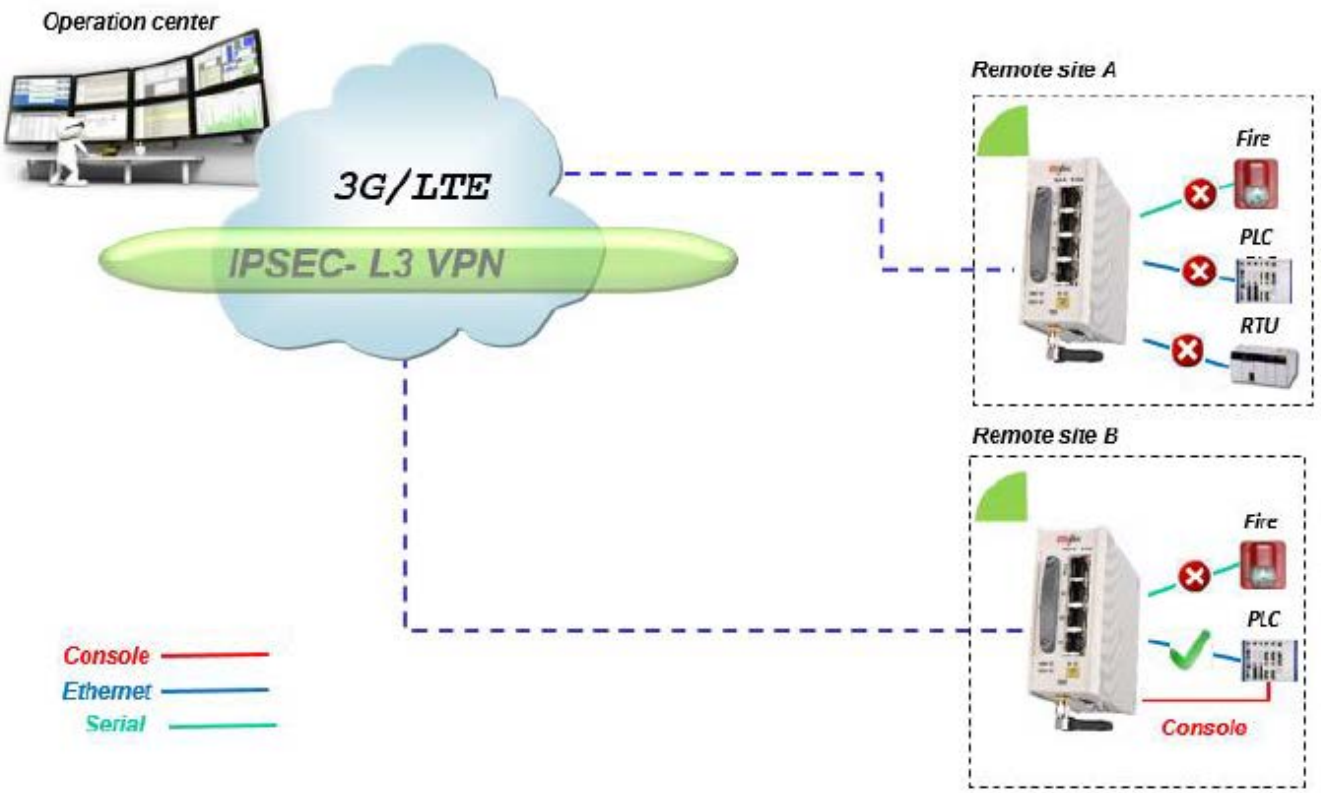
Source: Company data

Exhibit 14: Secure Gateway for Substations



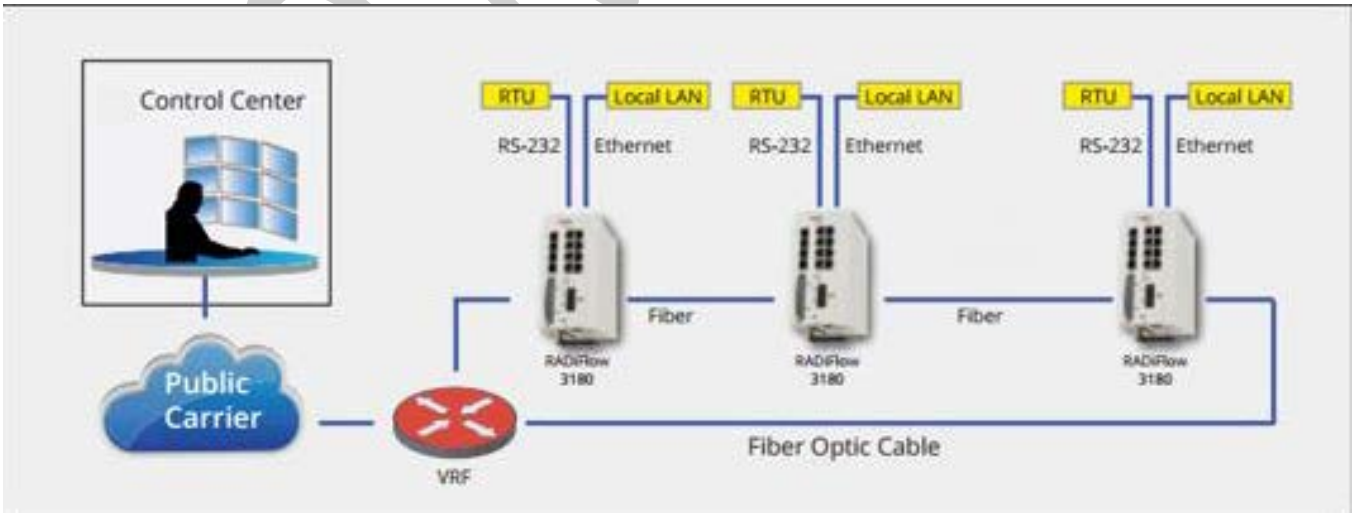
Source: Company data

Exhibit 15: Secure Remote Maintenance over Cellular



Source: Company data

Exhibit 16: SCADA Monitoring for Oil and Gas



Source: Company data

Exhibit 17: – Competitors in the Security Solutions Market

FortiNet

Fortinet Inc. provides cybersecurity solutions for enterprises, service providers, and government organizations worldwide. The company offers FortiGate physical and virtual products that provide various integrated security and networking functions to protect data, applications, and users from network- and content-level security threats; the FortiManager product family to manage the system configuration and security functions of multiple FortiGate devices from a centralized console; and the FortiAnalyzer product family, which enables the collection, analysis, and archiving of content and log data generated by its products. It also offers FortiAP secure wireless access points; FortiWeb, which provides security for Web-based applications; FortiMail for multi-featured messaging security; FortiDB for centrally managed database-specific security; FortiClient, an endpoint security product for desktops, laptops, and mobile devices; FortiScan for endpoint vulnerability assessment and remediation; and FortiSwitch Ethernet switches. In addition, the company provides FortiBridge bypass appliances to help ensure network availability; FortiAuthenticator for scalable secure authentication for enterprise networks; FortiADC for optimizing the availability and performance of mobile, cloud, and enterprise applications; FortiSandbox for detecting and mitigating advanced persistent threats; FortiCache to reduce the cost and impact of cached Internet content; FortiDNS for secure domain name system caching; FortiDDoS for protection against distributed denial of service attack; and FortiVoice for business telephone communication. Further, it offers security subscription, technical support, training, and professional services. The company founded in 2000 had $770 million sales in 2014 and is headquartered in Sunnyvale, California.

Check Point Software Technologies Ltd.

With $1.5 billion yearly sales Check Point Software Technologies Ltd. is the leader of the IT security market. The company develops, markets, and supports a range of software, combined hardware, and software products and services for information technology (IT) security worldwide. It provides network security gateway software blades and appliances that enable its customers to implement their security policies on network traffic between internal networks and the Internet, as well as between internal networks and private networks that are shared

with partners; and endpoint security solutions, which provide various software blades that run on individual computers connected to the network, such as desktop and laptop computers, as well as other mobile devices. It also offers security management solutions to ensure consistent operations in accordance with an enterprise's security policy, as well as SMART-1, a security management appliance that combines functionality, and storage and turn-key deployment into a single device. In addition, the company offers technical services, such as technical customer support programs and plans; certification and educational training; and professional services in implementing, upgrading, and optimizing products comprising design planning and security implementation services. Further, it provides ZoneAlarm solutions that protect consumers from hackers, spyware, and identity theft. The company serves enterprises, service providers, small and medium sized businesses, and consumers. Check Point Software Technologies Ltd. sells its products and services through a network of channel partners, such as distributors, resellers, value-added resellers, system integrators, and managed services providers. The company was founded in 1993 and is headquartered in Tel Aviv, Israel.

PaloAlto

Palo Alto Networks, Inc. serves the enterprise network security and endpoint security markets worldwide with firewall systems, unified threat management, Web gateway, intrusion detection and prevention, specialized threat analysis and protection, virtual private network, and enterprise endpoint security technologies. Its Panorama is a centralized security management solution for the control of appliances deployed on an end-customer's network as a virtual or a physical appliance; and its virtual system upgrades are available as extensions to the virtual system capacity that ships with the appliance. It also offers subscription services, such as threat detection and prevention, URL filtering, laptop and mobile device protection, malware and threat protection, and windows-based fixed and virtual endpoints protection services; support and maintenance services; and professional services, including application traffic management, solution design and planning, configuration, and firewall migration services, as well as education services. Palo Alto Networks, Inc. primarily sells its products and services through its channel partners, as well as directly to end-customers operating in various sectors, including education, energy, financial services, government entities, healthcare, Internet and media, manufacturing,

the public sector, and telecommunications. The company was founded in 2005, had $739 million sales in 2014 and is headquartered in Santa Clara, California.

Belden Inc.

$2.3 billion, Belden Inc. was founded in 1902 and is based in St. Louis, Missouri. It designs, manufactures, and markets signal transmission solutions for use in broadcast, enterprise, and industrial applications worldwide. The company's Broadcast Solutions segment offers production, distribution, and connectivity systems for the television broadcast, cable, satellite, and IPTV industries. Its products include camera mounted fiber solutions, interfaces and routers, broadcast and audio-visual cable solutions, monitoring and playout systems, outside plant connectivity products, and other cable and connectivity products. Its Enterprise Connectivity Solutions segment provides network infrastructure solutions for enterprise customers. This segment offers copper and fiber network systems consisting of cable, assemblies, interconnect panels, and enclosures; and intelligent power, cooling, and airflow management hardware and software for mission-critical data center operations. The company's Industrial Connectivity Solutions segment provides infrastructure components and connectivity systems for various industrial automation applications. Its products comprise industrial and input/output (I/O) connectors, industrial cables, IP and networking cables, I/O modules, distribution boxes, customer-specific wiring solutions, and load-moment indicator systems, as well as controllers and sensors for the mobile crane market. Its Industrial IT Solutions segment offers mission-critical networking systems, such as security devices, Ethernet switches and related equipment, routers and gateways, network management software, and wireless systems for customers in energy, automotive, transportation systems, and automation supplier markets. Belden Inc. sells its products to distributors, original equipment manufacturers, installers, and end-users.

Belden offers a variety of solutions through its brands, some of which were acquired through M&A. The brands include Belden Wire and Cable, Lumberg Automation, GarrettCom, Hirschmann Automation and Control, and Tofino Security, as well as various market solutions including Rail System Solutions, Automotive Manufacturing, and Substation Solutions. [??it isn't

clear what these market solutions are. Are they brands, or just areas in which Belden operates? Maybe you can delete them??]

Belden acquired Tofino Security as part of its strategy to enter the ICS security market. The company provides industrial network security products that are simple to use and do not require plant shutdowns. Its flagship product, the Tofino Industrial Security Solution, protects industrial networks from external cyber threats and internal network incidents. It facilitates the implementation of Plug-n-Protect zones of security for equipment with common safety requirements, as recommended in ANSI/ISA-99 standards. Tofino Security products are used by the process control, SCADA, manufacturing and automation industries.

Siemens

With almost $80 billion sales in 2014, Siemens AG is a global electronics and electrical engineering company. It was founded in 1847, and is headquartered in Munich, Germany.

The company's Power and Gas segment offers gas and steam turbines, generators, compressors, and power plant solutions for gas-fired plants, as well as solutions for power plant instrumentation and control. Its Wind Power and Renewables segment provides wind turbines; and implements turnkey projects for small hydropower plants. The Power Generation Services segment offers service support, maintenance, repairs, replacements, modernizations, and upgrades for gas, steam, and wind turbines, as well as generators, power plants, and compressors; and remote monitoring and diagnostics services. Its Energy Management segment provides facilities and systems for the low-voltage and distribution power grid level, smart grid and energy automation solutions, power supply for industrial plants, and high-voltage transmission systems. The Building Technologies segment offers fire safety, security, building automation, heating, ventilation, and air conditioning solutions, as well as energy management products and services. The Mobility segment provides operation management systems for rail and road traffic with solutions for airport logistics, postal automation, and traction power supply, as well as rail vehicles for mass transit, regional, and long-distance service. The Digital Factory segment offers integrated hardware, software, and technology-based services for manufacturing companies. TheProcess Industries and Drives segment offers automation, drive technology, industrial software, and services. The company also provides commercial finance,

insurance, asset management, project and structured finance, venture capital, and treasury services, and medical imaging, laboratory diagnostic, and healthcare IT solutions, as well as holding equity investments.

The Siemens RUGGEDCOM line of products provides a level of robustness and reliability for communications networks deployed in harsh environments. RUGGEDCOM products offer extreme temperature range, Zero-Packet-Loss technology for immunity to high levels of electromagnetic interference, and enhanced Rapid Spanning Tree Protocol (eRSTP™) for ultra-high-speed network fault recovery. RUGGEDCOM products can be found in mission critical networks used in substation automation, self-healing power grids or "Smart Grid" systems, intelligent transportation systems for traffic management and railway control systems, as well as in process control and manufacturing automation systems used across multiple industrial sectors.

RUGGEDCOM CROSSBOW is a proven secure access management solution designed to provide NERC CIP compliant access to Intelligent Electronic Devices. The RUGGEDCOM CROSSBOW solution focuses on delivering productivity gains for administrators and users while achieving full NERC compliance in managing, securing and reporting on remote access. The combination of the CROSSBOW Secure Access Management server and CROSSBOW Station Access Controller for local substation access form an integrated, comprehensive solution with a seamless configuration environment.

The Siemens RUGGEDCOM CROSSBOW application addresses the need for utilities to interactively access remote field IEDs for maintenance, configuration, and data retrieval. RUGGEDCOM CROSSBOW allows a native IED application to remotely communicate with its associated IEDs, as if the user were directly connected to the IED with a serial cable or network connection. User access is governed by the appropriate authentication model (e.g. RSA SecurID) and all user activity is logged and reported per the NERC CIP specification.

General Electric

General Electric (GE) operates as an infrastructure and financial services company worldwide. The company's Power and Water segment offers gas, steam and aeroderivative turbines, nuclear reactors, generators, combined cycle systems, controls, and related services; wind

turbines; and water treatment services and equipment. Its Oil and Gas segment provides surface and subsea drilling and production systems, equipment for floating production platforms, compressors, turbines, turboexpanders, reactors, industrial power generation, and auxiliary equipment. The Energy Management segment offers plant automation hardware, software, and embedded computing systems, including controllers, embedded systems, advanced software, motion control, operator interfaces, and industrial computers. The Aviation segment offers jet engines; aerospace systems and equipment; and replacement parts and repair and maintenance services for commercial and military aircraft, marine applications, and executive and regional aircraft. The Healthcare segment provides medical imaging, software and information technology (IT), patient monitoring and diagnostics, drug discovery, biopharmaceutical manufacturing technologies, and performance improvement solutions. The Transportation segment offers freight and passenger locomotives, and diesel engines for rail, marine, and stationary power applications; railway signaling and communications systems; underground mining equipment; motorized drive systems; IT solutions; and replacement parts and value added services. The Appliances & Lighting segment manufactures home appliances and lighting products for commercial and industrial applications. The GE Capital segment offers commercial loans and leases, fleet management, financial programs, credit cards, personal loans, and other financial services.

As part of the solutions for security in the infrastructure world GE offers CyberSentry™ SEM Security Event Manager. This is the GE's cyber security management and monitoring system, specifically designed to help utilities and energy intensive industrial companies manage security risks. CyberSentry monitors for. If it detects a configuration change or a cybersecurity issue, the system alerts operators using its industry standard syslog technology. With an intuitive interface and customizable reports, CyberSentry SEM helps users prepare for NERC CIP audits.

The company was founded in 1892 and is headquartered in Fairfield, Connecticut. In 2014 it had 305,000 employees and a turnover of $148 billion.

ABB

ABB is a 131-year-old company based in Zurich. With a yearly turnover of $40 billion and over 140,000 employees, it is a leading global player in its field, providing power and automation technologies for utility and industrial customers worldwide. The company's Discrete Automation and Motion segment provides motors, generators, variable speed drives, programmable logic controllers, robots and robotics, solar inverters, wind converters, rectifiers, and excitation systems, as well as power quality and protection solutions, electric vehicle fast charging infrastructure solutions, components and subsystems for railways, and related services for discrete automation, process industries, transportation, and utilities. Its Low Voltage Products segment provides protection, control, and measurement for electrical installations; enclosures, switchboards, electronics, and electromechanical devices for industrial machines and plants; products for wiring and cable management, cable protection systems, power connection, and safety; and building control systems for home and building automation. The Process Automation segment develops and sells control and plant optimization systems, automation products and solutions, and industry-specific application services for the oil, gas, petrochemicals, metals and minerals, marine and turbocharging, pulp and paper, chemical and pharmaceuticals, and power industries. The Power Products segment offers circuit breakers, switchgears, and capacitors, as well as instrument, power, distribution, and traction transformers for electrical and other infrastructure utilities, as well as industrial and commercial customers. The Power Systems segment provides transmission and distribution systems, as well as power plant automation and electrification solutions, including monitoring and control products, software and services, and components for power generation, transmission and distribution utilities, and other infrastructure utilities, as well as other industrial and commercial enterprises.

Waterfall Security

Based in Israel, Waterfall Security Solutions Ltd. is a leading provider of strong network security products which protect the safety and the reliability of control system networks. Aiming to eliminate the use of firewalls in critical infrastructure control systems, it develops products that provide stronger-than-firewall protection for industrial control networks. Waterfall claims that its innovative products dramatically reduce the cost and complexity of compliance with NERC-

CIP, NRC, NIST, CFATS and other regulations, and include support for leading industrial applications, including the OSIsoft PI™ Historian, the GE Proficy™ iHistorian, Siemens SIMATIC™/Spectrum™ solutions and GE OSM™ remote monitoring platforms, as well as OPC, Modbus, DNP3, ICCP and other industrial protocols. However as their solution is based on one-way communication it is quite limiting in terms of operations and is mainly used for segmenting between the IT and OT networks rather than securing the distributed OT network.

Waterfall products are deployed in utilities and critical national infrastructures throughout North America, Europe, Asia and the Middle-East.