PROSEGUR

cipher
a PROSEGUR company

The Convergence of Physical and Digital Risk Management

THE CONVERGENCE OF PHYSICAL AND DIGITAL RISK MANAGEMENT

SECURITY AND RISK

The physical and digital worlds are intertwined. A single provider can secure both. This white paper will go into the concepts surrounding security, threats, and risk. The paper will look at examples of past incidents, the benefits of close collaboration in physical and information security, and how Prosegur and Cipher deliver on these benefits and reduce risk.

“Risk and risk management are very much part of what keeps CEOs and the Board of Directors awake at night. In the 21st century risks can come from many different sources. Risk can originate from internal sources or externally from a spectrum of threats, such as organized crime and hackers. Technology, virtualization, globalization and the mobile work force have made all of the assets of the enterprise more accessible to bad actors,” said Prosegur Global Risk Services CEO Robert Dodge.

Security is the state of being free from danger or threat. Both humans and their possessions could be secure or insecure. Insecurity is vulnerability to threats to their rightful existence. There is a risk that a situation will result in security being broken, and thus a danger or threat occurs. Managing that risk is important.

To obtain security and reduce risk, people and the organizations they are part of do many things. Eventually organizations evolve and outgrow the security controls they once had. They go from having unlocked doors to sophisticated access control systems and IP video management systems at their disparate facilities globally. Security Officers are brought in to provide physical security services. Video cameras add increased situational awareness and help to extend the reach of security officers and can provide increased surveillance and detection of threats. Cybersecurity software and services protect the networks of an organization. The whole of all these activities constitutes a complete 360° holistic risk mitigation posture for enterprises in the 21st century.

Enterprises that take a converged approach to mitigate risk reap a wide range of benefits. There is better alignment of security strategy, enhanced communication, and more sharing of best-practices. Cooperation between physical and cyber security teams enables security staff to become more well-rounded and gain more visibility and influence with the c-suite and board.

VIRTUAL AND REAL-WORLD THREATS CONVERGING

“The hallmark of effective risk management is how effectively enterprises manage access control both physically and digitally. Today’s 21st century sophisticated threats leverage both physical and digital approaches in combination to achieve their goals. For example, a social engineering ploy by an individual at a lobby access point designed to deceive and gain access could be supported by a counterfeit badge produced by digital technology, or the access system could have been hacked to support the attempt,” said Dodge.

Converged physical and digital risks are enhanced greatly by the potential of impact and damage to an enterprise that can be caused by the insider threat with access. Negative impacts from converged risks manifest in the area of corporate espionage, sabotage and fraud.

Cybersecurity threats are impacting the real-world in many ways. This can be in the form of computer shutdowns that throw off real-world activity or direct impacts on devices that are connected to the Internet. Devices connected the Internet, also known as IoT (Internet of Things) devices, are everywhere. For consumers, this is in the form of Internet-connected appliances, video cameras, and even their cars. For businesses, IoT devices power critical systems for production and business functioning.

Mere information can result in a physical security threat. Recently, the trains systems in Iran were thrown into chaos by a hacker posting inaccurate messages on the digital signage at train stops in the country. Although the trains were not impacted, the people who viewed the messages reacted and a physical impact happened.

Stuxnet was the first and most brazen example of a digital threat manifesting in the real-world happened in 2010 also in Iran. A simple USB plugged into a computer had malware on it. The malware was designed to trigger only when connected to an industrial device involved in nuclear enrichment. The malware derailed the nuclear weapon program of the country. This incident was the first to open the world’s eyes to the convergence of cyber and physical threats. Other highlights of recent cyber-attacks with big real-world impacts are below.

Colonial Pipeline

Cyber Impact

On May 7, 2021, Colonial Pipeline fell victim to a cyber-attack. Shortly after the attack, the company paid a ransom in Bitcoin ransom totaling $4.4 million. The group responsible was likely a Russian hacking group DarkSide.

The attack appears to have started with a phishing email. Next in the attack chain was a ransomware infection. When this happens, the infected company cannot decrypt their computers. The hackers threatened to release the stolen code if a ransom was not made. Even if there was a backup of the encrypted systems, a data breach can do significant damage.

Real-World Impact

In order to contain the attack, the company shut down their operations until May 12, 2021. During this time, the media reports surrounding the attack began to report. This spurred massive runs on different gas stations, as people feared they would be without gas. Areas without reliance on the actual pipeline even reported shortages resulting from the panic.

Gas prices rose following the attack. Nationwide, the price of gas rose to a six year high. In some southern states, the prices rose 20% before and after the attack. The attack underscored the threat to critical infrastructure that cyber-attacks bring. A single hacker gang or even a single person can cause huge real-world disruptions.

Future Prevention

Intelligence on the hacker gang targets and techniques would have made the company better prepared. Different methods could have stopped the attack from happening, once launched. A phishing-delivered ransomware attack will not succeed if a person does not engage with the email. This human element to cybersecurity can be improved with training.

If Colonial Pipeline would have used different technologies, the malicious payload might not have been delivered. Email security software scan messages for signs of suspicious links. Even if a link is clicked, there is functionality that crawls the destination URL for signs of malware. Certain tools can stop a program that is not trusted from running.

Florida Water Treatment Plant

Cyber Impact
On February 5, 2021 unknown criminal hackers gained access to the Supervisory Control and Data Acquisition (SCADA) system of a Florida water plant. The hackers accessed the water plant remotely by using the popular Team Viewer program. To get access in the first place, they likely used compromised credentials. After noticing the compromise, the operators took steps to shut hackers out.

Real-World Impact
The attackers increased the amount of sodium hydroxide in the water treatment process. The attack did not have any real-world impact because the operator at the computer noticed the change and fixed the levels as soon as he noticed. The incident gained wide attention and served as an example of how cyber-attacks could be used for not just financial gain, but also to inflict physical harm.

Future Prevention
The incident serves as an example for many preventable cybersecurity blind spots. Analysis of the attack showed that “all computers shared the same password for remote access and appeared to be connected directly to the Internet without any type of firewall protection installed.” TeamViewer and software like it can be abused.

BENEFITS OF CLOSER COORDINATION OF SECURITY

Unified Intelligence and Action

A threat to one part of a company is a threat to the whole company. Working with a single provider with converged security solutions can eliminate the risk of independent silos and threat actions not being seen through one pane of glass will enhance risk mitigation intelligence and capabilities for the enterprise. The Risk Operations Center (ROC) is the hub for this intelligence. For example, the reports that come from an access control system might be correlated to physical threats but also can be repurposed to correlate to insider threat activity around information loss threats using technology. Video surveillance might be helpful to identify who was using a computer at a certain time to assist in a corporate espionage investigation.

Threats to the physical operations of an organization often start with digital indications. Criminals communicate in different channels that can and should be monitored both physically and digitally. Dark Web forums and marketplaces are where illegally obtained information and credentials are sold. Even social media like Facebook or Twitter can be monitored for signs of threats.

If there is a single organization-wide intelligence capability, the information can flow freely. A threat to a company CEO might surface on social media. Rapid assessment of the viability of the threat can be done by the intelligence team leading to timely notification that leads to heightened security awareness and potentially enhanced protection of the company CEO.

Having a converged robust single source of intelligence can help awareness and mitigation at different company departments. As an example, if a person gets a phishing email to wire money to a vendor, he reports that to IT. In this case, the finance department should also be aware as well as corporate security who can engage with law enforcement.

The sources of intelligence and coordination are integrated within ROC. A ROC can gather data on different threat streams both internal and external, analyze the threats based on existence, capability and intent, and then direct a variety of different security operations/responses as a result. The ROC of today takes in massive amounts of information from different sources, analyzes the information, and enables analysts to take steps to manage and reduce risk.

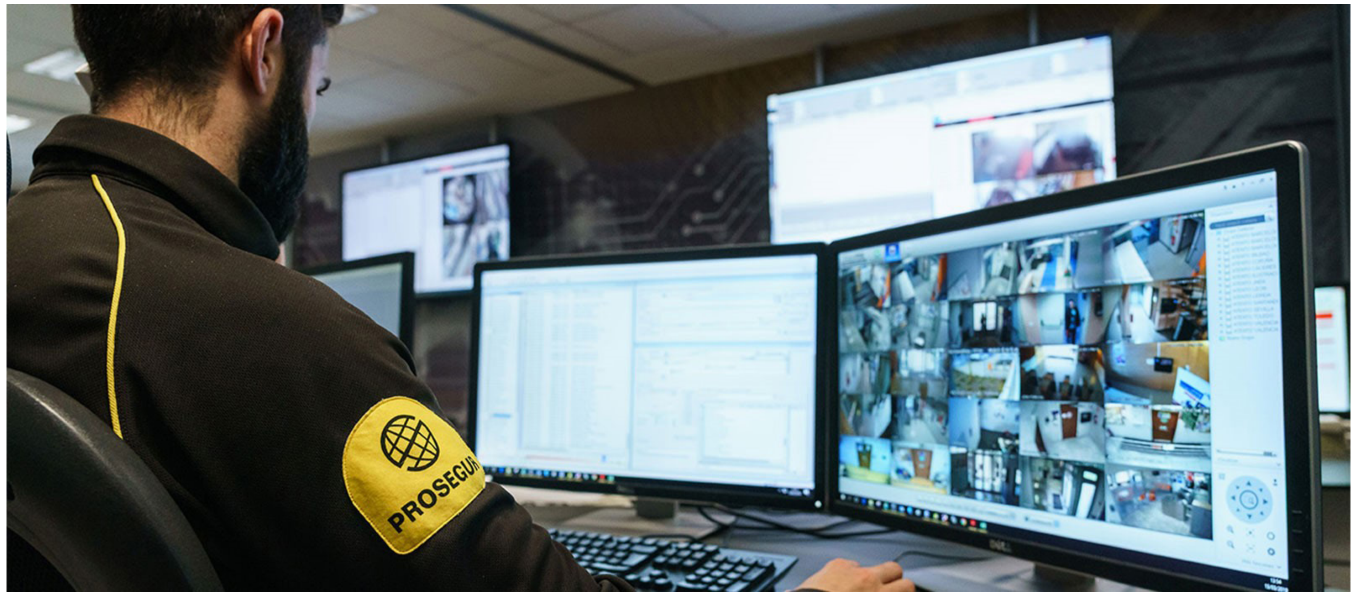
The ROC of the 21st century can go beyond security and risk. A ROC might monitor video feeds for the purposes of ensuring safety of people or assets, supporting global supply chains, gathering business intelligence on customer behaviors, and supporting business continuity of the enterprise. Business processes can be measured and tracked. Temperature or weather conditions can be factored in.

In the cybersecurity sense, the people in the ROCs are monitoring computer logs, responding to cyber incidents, and analyzing threats. Incorporating the political or economic risks can give even farther-reaching intelligence. These operations can occur in the same physical location or remotely. Sharing and using the combined information is the critical element.

Optimize Roles and Responsibilities

The Board of Directors and CEO are responsible for the welfare and governance of the enterprise. They charge others with handling the execution, strategy and details. The World Economic Forum says, "The board should encourage and empower its management team to create a culture of collaboration for the effective oversight, monitoring and control of ecosystem-wide risks."

The people responsible for reducing business risk and enhancing security must consider the different vectors a threat can come from. Having a single command structure can aid in incident response. Coordinating the overall crisis management response inclusive of media, physical response, and digital mitigation efforts are easier when the structure is unified.



At the levels of upper management, the knowledge of risk is more important than any knowledge related to a specific tool or tactic. Thus, there might be a single leader who is responsible for both the physical and digital security. Job titles of the present and future that fit this vision include Chief Security Officer, Chief Risk Officer, and VP of Security.

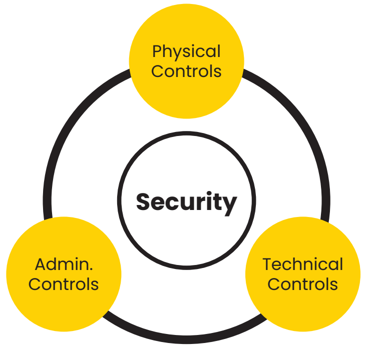
CSO Online says that "The CSO is the executive responsible for the organization's entire security posture, both physical and digital. CSOs also frequently own or participate closely in related areas such as business continuity planning, loss prevention and fraud prevention, and privacy." The industry is shifting from segmented security roles to a single decision maker for physical and digital security.

Having a better system of responsibility is related to eliminating unnecessary elements of a company's security posture. In some cases, there might be duplicate roles that can be combined with a unified structure.

Working with a single company to provide security reduces the Total Cost of Ownership (TCO). Cost savings can be made by optimizing roles and resources, whether a company is doing internally or contracting to an outside vendor. The cost of computers, Internet, furniture, real-estate, and other incidental costs are reduced when using a single structure.

Spending on enterprise security tends to be fragmented in organizations. Convergence in corporate security organizational management varies between 13% to 30%, according to a study done by ASIS International, so there is still a long way to go. The impact of not mitigating risks, whether they are physical or logical, is increasing. Contracting fragmented solutions tends to be highly complex, costly, hard to manage, and with that, the risk tends to increase.

Maintain Defense in Depth



The concept of defense in depth means adding different layers of security to reduce the risk to an organization's valuable assets from threats. The concept is sometimes talked about relating only to information security tactics. Adding the physical layer to the framework helps to give more context.

Physical Controls

Anything outside of the IT systems are classified as physical controls. This includes perimeter security such as fences and signage. Access control systems, intrusion detection systems, video surveillance systems and the guard force security are also part of the security in depth concept. All these components should be aligned to detect and respond to a potential risk to the organization. Cameras that monitor the grounds can aid in keeping areas secure by identifying suspicious behavior and predesignated activities supported by analytics. Physical controls are the most obvious for an organization and can signal deterrence to a potential threat. They can deter, detect, delay, and enable response elements to physically stop people from entering facilities or doing activities that are physically apparent. Physical security systems can integrate with technical controls to gain intelligence on early indications and warnings of threat activity.

Technical Controls

Technical controls include the hardware and software of a computer system. These controls factor heavily into managing and reducing an organization's risk. This is where cybersecurity tools come into play. Tools like Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), Next-Generation Antivirus (NGAV) can stop threats but require a specific skill set to properly use. Cipher is the Cybersecurity Division of Prosegur. They have dedicated employees who work 24x7x365 to use these technical tools to protect companies.

Administrative Controls

Training and policies are part of the administrative controls. Best practices related to administrative controls include never clicking links on suspicious emails, using complex and unique passwords, and being cautious with the information shared. The processes that are laid out for proper use of company equipment and are an administrative control. Requiring visitors to a facility to have badges and fill out a form is another administrative control that can reduce risk and increase security.

Employing excellence in all three areas of controls puts organizations in a secure position. For example, a company might constantly fall victim to ransomware due to poor administrative controls, where people click links that they should not. A social engineer can get past physical controls and get into a facility in order to steal information and then take advantage of technical deficiencies.

PROSEGUR INTEGRA

Prosegur Integra combines each part of the security landscape. Integra is a holistic approach to security that blends technology with the human expertise to achieve higher security at a lower cost to clients.

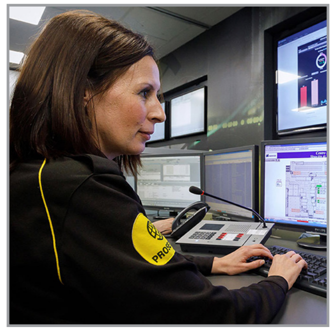
The solution encompasses:

People

Skilled security professionals are at the heart of Integra. Their roles could be on-site security officers, mobile officers, remote officers, monitoring agents, security operations center operators, supervisors, security technology specialists (technical architects, maintenance and support specialists, data analysts, cybersecurity experts, supervisors).

Technology

The right tech increases efficiency and reduces risk. The technology that makes up Integra can include access control systems, thermal CCTV, drones, enterprise security software, remote video storage, remote detection of safety conditions, and new AI-based capabilities that face recognition to anticipating incidents based on data.



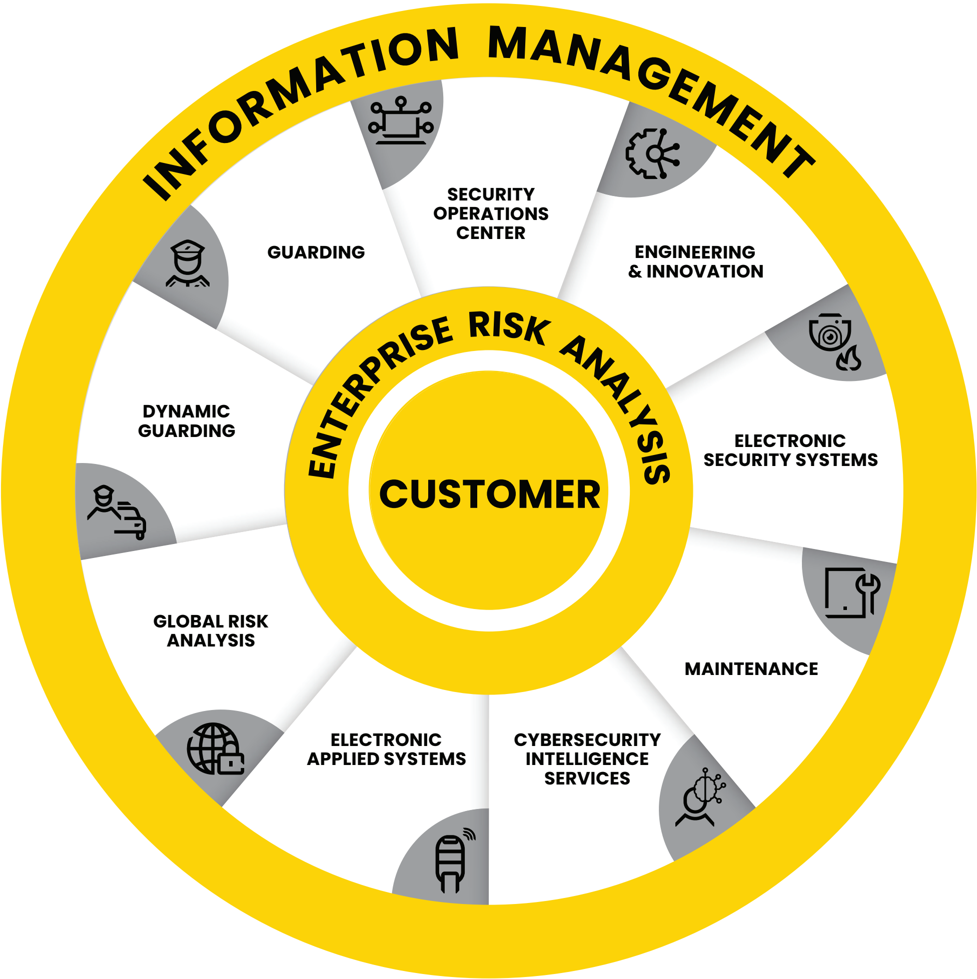
Processes

Orchestrating best-in-class technology and security professionals is the final component. Integra solutions include thoughtful processes based on company policies, local regulations, and best practices, with an end-to-end approach. Processes need to ensure that the overall operation is not fragmented.

Integra Visualized

An integrated enterprise security solution is not about technology taking over human roles. It is about enhancing the capabilities of what people, technology and processes can accomplish in a comprehensive and tightly-coupled approach.

For example, guards need to have two-way communications with the SOC, so an AI-based analytics engine may trigger a mobile guard to take preventive action based on the likelihood of an incident.



Every day Prosegur helps organizations large and small solve their security challenges through technology, teamwork, innovation, and relentless customer focus.

PROSEGUR SOLUTIONS

Prosegur offers a complete suite of solutions for companies looking to enhance their physical and digital security. Key overall offerings are listed below. Organizations can utilize all the solutions together as part of Integra or choose what services fit for them. Prosegur can integrate different systems like include access control, CCTV, drones, watchtower, video management systems, maintenance, enterprise software integration, and more. Highlights from specific offerings are below.

Global Risk Services

Prosegur's Global Risk Consultancy division provides enterprise risk management solutions for clients globally including protective services, corporate investigations, risk consulting and intelligence services/risk operations Center (ROC) support Globally. The group develops customized risk solutions for clients across the globe. The solution helps improve operational performance, reduce risk, expand profitability and provide a greater return on investment.

Remote Video Monitoring

Prosegur's video monitoring solutions combine advanced surveillance cameras, video analytic software and live monitoring by highly trained agents to provide better security coverage for buildings. For sites that have audio announcement capability, monitoring agents can make live announcements to any persons trespassing or exhibiting other unwanted behavior. These "voice-downs" have been proven highly effective at stopping intruders without having to involve the police.

Guarding

People on the ground are an important element of any sophisticated security posture. Highly trained and vetted men and women can handle all sorts of security responsibilities. Prosegur security officers can provide security at airports, events, front-desks, and other venues. Dynamic guarding gives more flexibility since the guards use vehicles to expand the range.

Electronic Article Surveillance

Loss prevention in the retail sector depends on a range of activities. Guards might be at the front. Cameras could be overhead. A very effective way to prevent theft is Electronic

Article Surveillance (EAS) technology. Prosegur is a leading provider of tags, sensors, and related technologies.

Cybersecurity

Cipher is the Cybersecurity Division of Prosegur. Cipher offers an unparalleled range of tools and services for protecting companies against cyber threats. Specialists monitor activity 24x7 using cutting-edge cybersecurity software. Cipher helps companies with strategy to mitigate information security risks and improve compliance with relevant laws and frameworks. This all results in a reduced risk of falling victim to phishing, ransomware, and other cyber-attacks.

PROSEGUR

cipher
a PROSEGUR company

DOWNLOAD

cipher.com
contact@cipher.com