

cyberprotection

PROGRAM From *Tyco Security Products*

Six Part Approach to Cyber Protection of Physical Security Products

A Guide from the Tyco Security Products
Cyber Protection Team



Tyco Security Products Cyber Protection Program

Born from decades of providing critical solutions to the United States Government and other multi-national customers, Tyco Security Products' Cyber Protection Program is one of the industry's first programs to offer a holistic approach to cybersecurity for physical security products.

The **Cyber Protection Program** combines best practices in secure product development, testing and evaluation, configuration guidelines for compliance, and industry advocacy to help our

customers **protect physical security products** from attack, damage, disruption, unauthorized access or misuse.



Six Part Approach to Cyber Protection

Tyco Security Products' Cyber Protection Program of Physical Security Products looks beyond our individual components and devices.

The multifaceted program provides a **holistic** approach to cybersecurity awareness for physical security.



Secure Product Development Practices



Inclusive Protection



Configuration Guidelines



Rigorous Testing



Rapid Response



Educate and Advocate

Program Goals:

- To help reduce the risk of cybercrime and the resulting damages
- To support cybersecurity policies and frameworks that are driven by corporate IT Security Risk
- To give you confidence that we have minimized the possibility of introducing vulnerabilities into the Tyco Security Products' physical security systems you install

Raising the Bar

We've set the bar extremely high with our **Software House** access control solutions, **American Dynamics** video management systems, and **Illustra** IP cameras, and are committed to employing the same cyber safety mindset across other product lines within our product portfolio.

We've achieved a host of **industry firsts** that make us the solution of choice for businesses of all sizes looking for help in reducing their cyber risk.

- ✓ **FIRST FISMA-Ready** access control and video solution with C·CURE 9000, VideoEdge and victor
- ✓ **FIRST Federal Information Processing Standard (FIPS) 140-2** validated system with C·CURE 9000/iSTAR
- ✓ **FIRST Physical Access Control System (PACS)** Approved access control system with C·CURE 9000



Why the Focus on Cybersecurity?

Today's security professionals are faced with unprecedented threats to maintaining a secure environment for employees, visitors, and valuable assets.

For many, the days of worrying only about admitting/denying access and recording video are long behind them.

In fact, at a recent White House Summit on Cybersecurity and Consumer Protection, President Barack Obama raised an important paradox:

the very technology that can be used to do great good can also be used to imperil us and do great harm.

"Sooner or later, it touches every aspect of our lives, public and private, social and economic."

John Hennessy,
Stanford University President
Speaking at the White House Summit on Cybersecurity and Consumer protection on Feb 13, 2015



High Profile Breaches Bring Bright Spotlight

In 2008, an **oil pipeline in Turkey** exploded without triggering any alarms or sensors. It was not until 2014 that the press reported investigators had found that hackers had used a vulnerable security camera to gain access to the pipeline's network.

An unsecured camera that was there to protect the pipeline became the **weak link** that sabotaged operations resulting in millions of dollars in damage and lost revenue.



Israel's major traffic tunnel was hit by a massive cyber attack. One of the experts reported that it was a Trojan horse attack that led to **malfunctioning of a security camera** in the tunnels.

Sony Pictures, Target Corp, Anthem Insurance Inc.

With such high profile cybersecurity breaches, it is no surprise that cybersecurity is a top-of-mind issue for business leaders around the world.

How Relevant Is This To Your Business?

Businesses must have a continued focus on cybersecurity risk so they can maintain operations when a cyber incident occurs.

Leaders need to mitigate the risk of these threats from hackers, activists or malicious insiders and the resulting activities such as:

Sabotage: such as disabling systems or disrupting operations, potentially resulting in lost productivity and revenue;

Stolen personal data: such as financial or health information, potentially resulting in loss of customer trust, denigration of brand, and ultimately lost profits;

Stolen Intellectual property or trade secrets: ranging from marketing plans to research and development data that could result in financial losses and loss of competitive advantage;

Extortion (Data Ransom): where the company or individuals pay ransom to regain access to their system or data, and/or;

Regulatory action or negligence claims: such as penalties from a government agency or civil lawsuits

Some studies report that **three out of every four organizations have suffered at least one successful attack** in the past 12 months and more than half reported being infiltrated between one and five times during that period.

Looking Beyond the Components

With more and more physical security technology running on the network, installing systems that jeopardize your cybersecurity policies is the equivalent of leaving your doors unlocked.

However, **not all manufacturers' cybersecurity programs are equal**. Some offer protection on **single components** of a broader system, while others simply point to rudimentary hardening guides.





Secure Product Development Practices

Accidental design or implementation errors as simple as copying a buffer without checking the size of input can introduce vulnerabilities into software and firmware

The ease of inadvertently introducing weaknesses combined with the fact that **30 percent of companies never scan for vulnerabilities** drives the necessity for making secure development practices a key part of any cyber protection program.

At Tyco Security Products, our engineers are proficient in secure coding and testing procedures.

Beyond that, we've developed an autonomous **Cyber Protection Team**, an independent branch of the development team, with **authority** and **responsibility** of managing the development process and final product release, and monitoring compliance with our secure development **best practices**.

...62 percent of organizations have too few information security professionals. ...this decline is not about shortfalls in organizational budgets, but rather an insufficient pool of suitable/skilled candidates...





Inclusive Protection of Components and Systems

Many manufacturers concentrate on protecting their piece of the security pie, but **cybersecurity is more than device hardening**. It must also include the ability to secure systems with a range of capabilities to complement diverse security needs.

For example, a C-CURE 9000 and iSTAR access control system can be configured to support some of the most stringent controls necessary for secure network communication, including:

- End to End Encryption with SHA-2 & TLS
- Encrypted database communication
- System Auditing, Alerting and Management
- Denial of Service Protection
- Restriction of Ports, Protocols and Services
- Highly customizable user access & permissions
- Archive, failover & high availability





Configuration Guidelines for Compliance

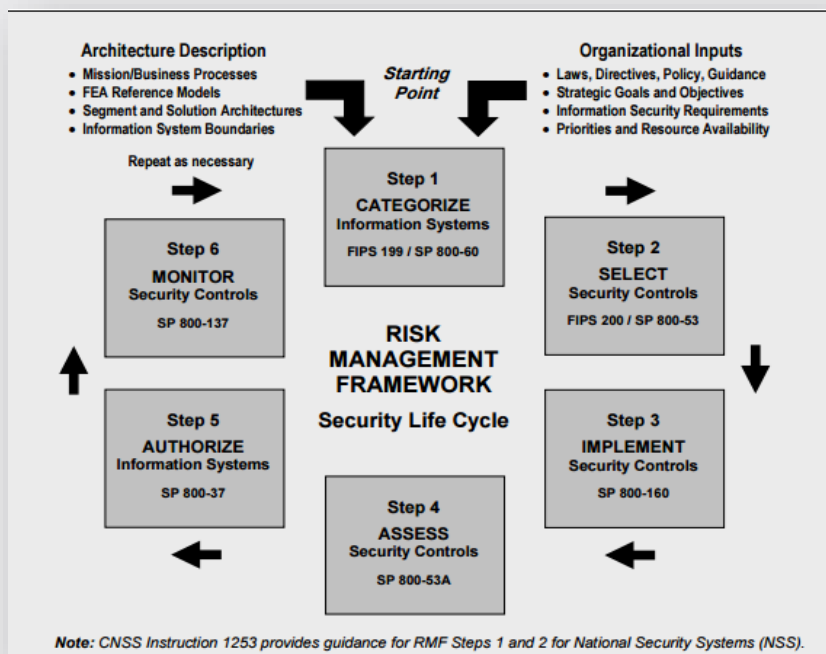
The Cyber Protection team provides comprehensive documentation to assist you in configuring C-CURE 9000, VideoEdge, and victor systems to comply with regulatory requirements.

For example, the team uses the **Risk**

Management Framework
from NIST 800-53

“Security and Privacy Controls for Federal Information Systems and Organizations” to help

users configure access control and video systems that require that high level of compliance.

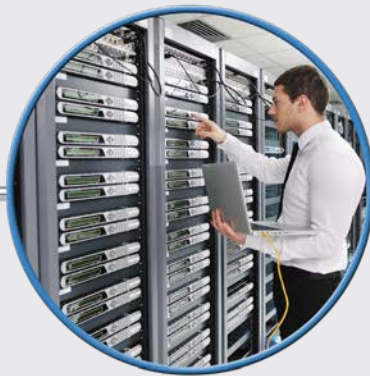




Ongoing Rigorous Testing

At Tyco, cybersecurity does not end when a product is released. The Cyber Protection team employs **rigorous, continuous testing** to minimize the risk of software updates and new configurations of our cyber program-compliant products introducing new vulnerabilities.

In addition to the testing conducted by the Cyber Protection team, **independent testing** is conducted annually on the products.





Rapid Response to Vulnerabilities

Tyco understands that a system secured today may become insecure tomorrow with the announcement of a new vulnerability. The Cyber Protection team is constantly monitoring a variety of sources, from the **National Vulnerability Database** to various media and professional sources to identify new vulnerabilities that may impact our cyber program-compliant products.

When such a vulnerability is announced, our Cyber Response team assesses and validates a resolution. This team is composed of dedicated engineers from product security, development, quality, and tech support.

This unique, **cross-functional** structure provides a thorough perspective that allows the team to quickly generate an advisory and follow up with fully qualified and tested patches.

The team was recently able to develop, test and release patches for critical vulnerabilities such as **Heartbleed** and **Shellshock** in just **two weeks**.



Advocate and Educate

We are passionate about the need for everyone involved with security to take the threat of cyber attacks seriously.

For Tyco, it has become part of the development culture and we are committed to helping our partners and customers understand what we are doing, how we are doing it, and how they can do their part to strengthen the security infrastructure.

In addition to maintaining critical training and development certifications, our Cyber Protection team travels the world, speaking and advocating for the rigorous protection of all security systems.

We have held education sessions at ISCW, PSA Tec, ASIS, and company events, hosted industry webinars for hundreds of security professionals, and published articles, white papers, and hardening guides.

tyco Security Products / Webinar /

Cybersecurity Readiness of IP-based Systems

What You Need to Do to Have Cyber Security Readiness of IP-based Systems

Hackers are using any means possible to infiltrate networks - even security products. That's why IT departments are now asking tough questions about manufacturers' cyber security programs.

Join us to learn the key components of an efficient cyber security program including:

- Vulnerability assessments
- Third-party penetration testing
- Strategies for improving response to threats

PLAY

William L. Brown Jr.
/ Sr. Engineering Manager /
/ Regulatory and Product Security /

tyco

Conclusion

Tyco Security Products Cyber Protection Program is an extensive and systemic approach to developing, configuring, and supporting our physical security products and systems that help you reduce the risks associated with cyber attacks. Please see the additional following resources:

Program Website

Visit often for the latest information and sign up to receive our Cyber Advisory Bulletins



Program Brochure

Easy 'print-and-go' overview of our comprehensive program



“Our understanding of [these] regulatory rigors has helped us better partner with our customers to more effectively mitigate these risks from hackers, activists or other malicious insiders when it comes to their physical security systems.”

Steve Carney

Senior Director, Integration Platforms, Tyco Security Products.



cyberprotection

PROGRAM From

Tyco Security Products

[LEARN MORE](#)