cyviz

How to build secure collaborative environments for the digital workforce

Building secure collaboration environments and control rooms with strict security requirements used to be the prerogative of Command and Control spaces. However, digitalization has entered the workplace of all industries, and with it the age of global connectivity. This implies that video conferencing, and content sharing have become an integrative part of conducting business. The need to collaborate with external partners and share sensitive data over networks has also become the new norm and has opened businesses to vulnerabilities. While control rooms used to be more locked down, they now must open to other lines of communications, demanding hence more secure measures. Business must understand that a proactive approach to security could save them from facing operational threats. The need for protecting critical infrastructure is more crucial than ever and calls for a new way of building and delivering collaborative environments. With the rise of cybersecurity attacks, and the decentralization of workforces, businesses are vulnerable and as a result, starting to request higher security standards. Recently, we have been seeing the rise of customers from industries such as Energy, Utilities, and Transportation requesting levels of security and information sharing capabilities, traditionally requested by Military and Defence organizations. These new requirements are now becoming the new building blocks of control rooms and large collaboration rooms.

Protecting business-critical infrastructure in multipurpose rooms

Businesses depend upon a set of operational equipment, information systems, networks and utilities to function and deliver value, are now understanding the importance of monitoring and protecting their own critical infrastructure. Think about production lines, drilling activities, air control traffic or financial transactions. Securing infrastructure requires the right technology partner. Businesses need to adopt resilient technology platforms that will shield them from critical infrastructure breaches, help predict potential outages and attacks by integrating and displaying in real-

time all relevant information feeds and content sources. To achieve this, organizations need to create multipurpose spaces where they can monitor and take action it in real-time.

Critical Infrastructure Components[1]	Typical Sub-components	Potential Information Security Issues
Operations	• production line equipment • warehouse operations • transport and logistics • financial processing equipment	Malware infection of production line control devices, tampering of ATM equipment
Tele communications	• data networks and landline • satellite • mobile communications equipment	Physical damage or theft of landlines, theft of intellectual property, telecommunications fraud, eavesdropping
Utilities	• water and gas pipelines • electrical supply • sewage treatment	Loss of power to flow-control devices, failure of UPS and/or standby generators, hacking of Supervisory Control and Data Acquisition (SCADA) devices
Buildings	• perimeter safety • gated access control and surveillance • environmental monitoring equipment	Loss of physical access to premises and internal areas of buildings, theft of assets, malicious damage to controlling equipment

Collaborating with external partners, securely

Companies are increasingly outsourcing operations, or their maintenance to third-parties and external partners. Oil and Gas organizations for instance form partnerships and joint ventures and need different companies to work side by side in the same environments with different levels of access and information restrictions. This means that network security policies cannot be compromised. For example, it should not be possible to use the computer general network connection for transportation of video, audio or US, and this connection may be beyond the main access. Furthermore, it would not be practical to insist that certain types of screen scraping software must be installed on each connected computer, as this challenge the IT policies of the company owning the computer. An IP based routing infrastructure for instance brings higher security and flexibility and ownership to the business, eliminating risk of bringing third parties to gain

[1] Table source: https://www.infosecurity-magazine.com/magazine-features/what-is-critical-to-your-infrastructure/

physical access to the networks. Cyviz has been working on a new generation of IP based infrastructure for routing and data distribution enabling different levels of access to information within the same organizations and with their external partners. The solution needed to be innovative and based on IT principles with a simple distribution through IP. By changing the signaling distribution and avoiding the rigidity of cabling and matrixes, this resulted in an 'information highway' allowing customers to handle and distribute all data, and information and to work on digital assets with much more flexibility.

Sharing (Big) Data assets over networks

More and more data are being scrapped, analyzed and shared; 40 trillion gigabytes of data by 2020[2] and around 97% of organizations are investing in big data and Artificial Intelligence[3]. 84% of enterprises have also launched advanced analytics and Big Data initiatives to accelerate their decisions making[4]. Big data has become both an opportunity and a potential threat.

The real challenge for computer systems in secure environments is to maintain confidentiality and integrity of data. Typically, there are two design approaches to manage issues like these; partitioning and restriction. Partitioning refers to the ability to dedicate resources within the system to isolated groups, with no chance of unintentional crossover, within a router, switch or system of routers and switches. Essentially, partitioning creates several routers within a router. Restriction addresses the idea of limiting access on a user-by-user, source-by source basis. A strong Keyboard Video Mouse system design will allow the system manager to determine which users gain access to which sources, and perhaps more importantly, which users are denied access to which sources. The result is a secure system architecture engineered from the ground up results in a scalable solution, which doesn't compromise the system administrator's ability to perform configuration management easily across the entire facility. The objective of physical separation is to prevent the threat (people) from physically accessing the content or the system. A common approach is to prevent unauthorized users from entering the physical location of the system, by restricting access through card readers, biometric readers, etc. The physical separation between Information Processing Units (IPU) of various classifications is maintained in a remote location(s) accessible by the system administrator and out of the way of the mission operator. This greatly minimizes attack vectors and the insider threat as compute resources and the IP network are no longer in the operating environment. In many instances, end users need to switch between two or more computers, with different classification levels, introducing data vulnerabilities.

Multiple corporate networks and multi-classification

Businesses are also working with multiple corporate networks, and another way to secure workflows and operations within collaboration rooms and control rooms is to provide the technology to support it. Multi-classification is another way to deliver the optimal security and access restriction required in secure environments. This approach differentiates between security levels as they apply to different individual clearances and different networks. This flexibility in network source configuration is a significant advantage in Cyber Security Operations centers, Joint Operations centers and in Command & Control environments where multi-level security is a requirement. Computer sources from different networks and security classifications can be securely connected to the system, so content from multiple sources can be combined into an optimal representation of mission-critical information. In many instances, end users need to switch between two or more computers, at different classification levels, introducing data vulnerabilities. Strict security rules for the protection of classified information dictate that data is processed solely in trustworthy red networks and never transferred to black networks, where unauthorized personnel would have access to it.

2 Source EMC
3 Source New Vantage survey 2018
4 New Vantage survey 2018

This is a common situation in the military and government control rooms. Normally data is required from different classification systems from public internet, restricted sources, Secret and up to Top Secret and beyond. Assurances need to be given that data cannot be transferred whether via fault condition, malicious actions or even by things like fortuitous conductance of signaling cabling. The worst-case scenario would be Above Secret data being visible on the internet.

Things that are done to remove the possibility of cross contamination of networks are:

- One-way diode signal paths
- Separation of signals into logical blocks corresponding to network they belong to
- Separation of source and destination cabling to not run in the same conduit or cable tray
- Separation of network cabling to not run in the same conduit or cable tray.
- Optical systems to remove electrical conductance of signals
- Robust control systems which control the availability of systems to destinations

Multiple security levels

More and more there is a requirement for companies to keep data siloed to their own network. Simple examples could be customer, bank and governing body or normal operation, exercise and control body all wanting to visually share information without having to connect networks or risk transference of data between systems. Cyviz solutions comply with the one-way-only video distribution and processing requirements found in environments with multiple security levels. This implies that content from one security level can never be accessed from sources on a lower security level. Equally, computer sources from different networks and with security classifications can be securely connected to the system so content from multiple sources can be combined into an optimal representation of mission-critical information, through one-way video to the wall. Cyviz' control rooms and operations centers are designed to adapt to staff accreditations and present content accordingly and move between pre-configured modes to enable classified sources when needed using the same system. With Cyviz technology it is possible to adopt solutions able to switch modes and security levels as the situation requires within one and the same environment. Content from one security level can never be accessed from sources on a lower security level. Additionally, computer sources from different networks and security classifications can be securely connected to the system, so content from multiple sources can be combined into an optimal representation of mission-critical information.

Sources

https://www.ey.com/en_us/oil-gas/how-digitalization-in-oil-and-gas-is-creating-security-risks

https://www.mckinsey.com/business-functions/risk/our-insights/critical-infrastructure-companies-and-the-global-cybersecurity-threat

http://www.cs.cornell.edu/andru/papers/sp03.pdf

https://techjury.net/stats-about/big-data-statistics

https://newvantage.com/big-data-2/

https://onlinedegrees.sandiego.edu/threat-or-opportunity-big-data-and-cyber-security/