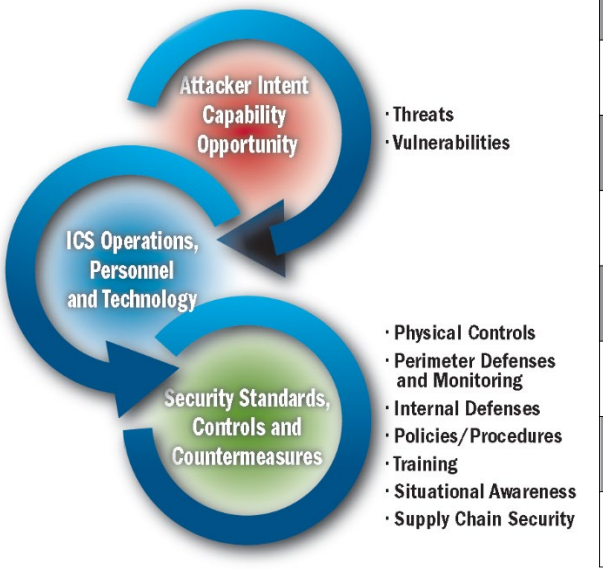
Journal Extras for May 2023

The following pages contain supplementary information for these articles in the May issue of *ASHRAE Journal*:

Cybersecurity for Building Automation Systems

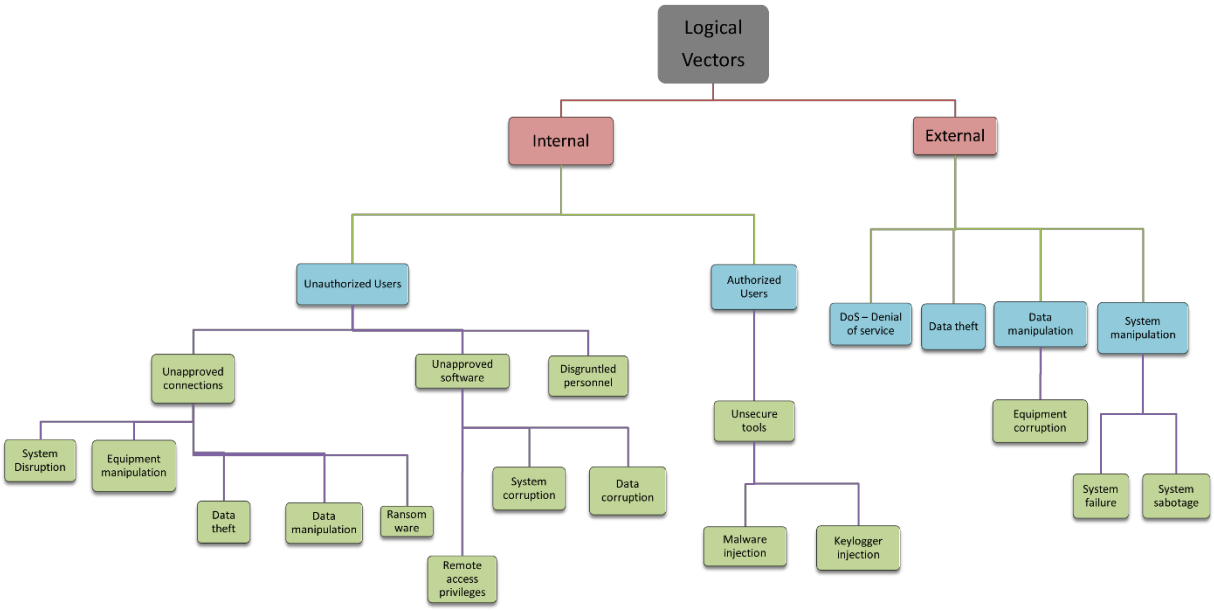
By Ron Bernstein, Member ASHRAE

Online Figure A



Defense in Depth Strategy Elements	
Risk Management Program	• Identity Threats • Characterise Risk • Maintain Asset Inventory
Cybersecurity Architecture	• Standards / Recommendations • Policy • Procedures
Physical Security	• Field Electronics Locked Down • Control Center Access Controls • Remote Site Video, Access Controls, Barriers
ICS Network Architecture	• Common Architectural Zones • Demilitarised Zones (DMZ) • Virtual LANs
ICS Network Perimeter Security	• Firewalls / One-Way Diodes • Remote Access & Authentication • Jump Servers / Host
Host Security	• Patch & Vulnerability Management • Field Devices • Virtual Machines
Security Monitoring	• Intrusion Detection Systems • Security Audit Logging • Security Incident & Event Monitoring
Vendor Management	• Supply Chain Management • Managed Services / Outsourcing • Leveraging Cloud Services
The Human Element	• Policies • Procedures • Training & Awareness

Online Figure B



Who Owns the Cybersecurity Plan?

Other Members of the Team:

Owners Representative

Clearly owners may not have the knowledge or ability to provide a full risk assessment nor might they have the ability to develop a BAS cybersecurity plan, prevention plan, breach plan, and any legal management. Owners may turn to a BAS design consultant well-versed in these issues and can act as the owner's representative when discussing design and implementation strategies and options. This consultant has the primary task of digesting the owners requirements into a BAS Framework while working with the project team to design and implement the best solution for the project. Having a team engaged to look after the owner's best interests is key to a successful strategy.

System Designer

From a technical aspect, it is the system designer and the specifications they create that will ensure the right level of security for each project. The BAS system designer must take on the important role of developing the engineering design and project specification and also work with many project disciplines. The BAS designer is typically part of a MEP (Mechanical, Electrical, Plumbing) Consulting Engineering firm that has embedded or subcontracted capability to effectively assess and design the cybersecurity plan for the facility. System designers dive into all of the integrated automation details for all building systems. They define the responsibilities for all contractors and coordinate the requirements and submittals. As we'll discuss, the BAS designer must account for all tiers of the project design from physical devices, programmable controllers, the network infrastructure, and the BMS front end. See the ASHRAE 4-Tier architecture map in the printed article.

IT Group

The facility IT department has a critical role as the gatekeeper between internal and external data and control system protection. Sometimes the IT group is part of the owner's staff, but this can also be contracted out to an IT firm to manage the project. Often the IT contractor has a direct, long-term relationship with the owner that extends beyond construction/retrofit. However, IT personnel cannot and should not be required to know all of the idiosyncrasies of building controls. A team approach is necessary with facilitation by the owner's representative to manage the design process.

Facility Engineering and Maintenance (FME)

The ongoing maintenance and monitoring of the systems falls into the facility engineering and maintenance team where breach alarms must be managed. This can be through the security system, the BMS front end, or a variety of other avenues depending upon the nature of the facility. The FME team has a significant role in defining the cybersecurity requirements for the project. As the front line team knowledgeable about the facility, the equipment, and the potential risks of a breach, they are key to defining and enforcing the plan.

Legal Counsel

Often an afterthought, engaging with a facility legal department early in the process can be extremely important. Legal counsel will understand the risks to the owner and how to manage them. Knowing what can happen to the physical facility is as important as knowing what can happen during a data breach. With increasing threats to critical infrastructure, operational cybersecurity is now front of mind

with lawyers, insurance companies, and legislators. Legal teams can help assess the value, importance, and risk mitigation plans, especially if an “event” does occur. Legal can also work with HR to enact the right levels of access privileges and maintain onboarding and offboarding of credentials.

Human Resources

Human resources departments help set policy and procedures for how people access the work environment. Onboarding and offboarding personnel are not only critical for the staff, but for contractors and 3rd parties. HR typically works closely with the IT team to set policies and their check and balance system to minimize internal threats.

Audit Team

An internal team that periodically reviews the current BAS cybersecurity implementations, establishes any new or revised requirements and makes adjustments to the plan.

Assembling a Cybersecurity Plan

Cybersecurity Plan Constraints

It's also important to assess any constraints that are not easily or cost effectively overcome. In some cases, identifying, documenting, and accepting a certain level of risk is all that can be done given certain constraints. This could be financial, resource, or time constraints. It is important to not ignore these constraints, but work within their limitations and develop an ongoing plan to help reduce or mitigate them.

Plan Resources and Execution

Defining the resources and the execution of the plan also requires the evaluation and assignment of responsibilities. They include:

- Personnel Responsibilities
- Management Responsibilities
- Contractor Responsibilities
- Consultant Responsibilities
- Supplier Responsibilities

Each entity engages with the project in their "scope of work." Cybersecurity should be added to this scope of work and clear roles and responsibilities identified and agreed to.

Oversight and Evaluation

Oversight and ongoing evaluation are also part of any good CS plan. Periodic enforcement evaluation, spot checking, testing of alarming and alerting protocols, hardness testing, system updates/patches protocols, and supplier product security assessments and evaluations are some elements of a good overall best practice plan.

Event Management

While not typically part of the overall BAS design process, understanding how to react to a breach should be part of any system design discussion. A cybersecurity BAS event could be an attempt to access a controller by entering in wrong credentials too many times, addition of an unauthorized computer based on its MAC address, access of the BMS from an unknown IP address, or an attempt to set the state of a controller to a value outside of its allowed limits. For the building systems and equipment, if an event occurs, good design practice is to ensure each system and equipment is programmed to locally manage any "out of range" actions imposed on it from external sources. This requires program logic to first identify all logical limits of any command, then put a check and balance into the program to ensure no outside message can put the system or equipment into an undesired state. This responsibility should be clearly identified in the design specification.

Notifications/Breach Procedures

If cybersecurity event does occur, defining a protocol for managing the event should also be put in place. With facility control systems, this includes how to manage the physical implications of an event, but there is also the communication, legal, and business responsibilities as well. Typically, the legal department will have "breach procedures" put in place. But often these are substantially more focused on the "data" side and less on the "physical" side of a breach. Having a clear line of authority, a

communication and reporting process in place, a tracking and tracing protocol, legal implications and a response protocol should be part of the overall plan.

Notifications, both internal and external, to key stakeholders and responsible parties in a timely, accurate, and data driven manner can help reduce the overall impact of an event. Key stakeholders for notifications include:

- Executive Management
- Facility Director
- Environmental Director
- Safety Director
- Corporate Security
- Emergency Response Teams (ERT)
- Operations Staff
- IT Staff
- Law Enforcement
- Data/System Owner/Responsible Party (Contractor/Supplier)
- Shareholders
- Customers/Owners/Public

Design Principles

Desired Outcomes

When specifying the cybersecurity requirements for a facility it is best to start with what is needed for the type of facility; the desired outcomes. A full site assessment of the level of risk, mitigation plan, affected systems and components, and the budget. Don't forget the budget. Cybersecurity requirements can balloon a capital project budget in no time if the desired outcomes are beyond the facilities ability to meet them. Develop a clear "fit for purpose" model of the needs of the facility based upon the various risk factors. Example risk factors include access to privacy data, access to process data, access to personnel location information, access to equipment overrides, facility disruption, and the big one, crossover intrusion or "pivoting" from the BAS to other facility systems such as data center, life safety, point of sale, and human resource personal data.

Continuous Monitoring

One best practice for helping secure building systems is to build in continuous monitoring of the various threat vectors in the base system design. Simple monitoring of communication systems for anomalies can provide a rapid response mechanism for facility managers. Often systems are not designed with any network traffic monitoring. When a breach occurs, it may be hours, days, or weeks before anyone realizes it, and the damage is done.

Anomalies might be things like unauthorized access request/denial, network parameter change requests that are out of range, too many messages from one source (a typical DOS – denial of service attack) that attempts to compromise the system by overloading the network. Consider designing in the requirement to monitor and log all data traffic on the control network(s) for archival purposes. Tools to distinguish between normal network traffic versus unusual traffic can be beneficial in helping manage data overload. Consider the model CCTV video surveillance systems have operated in the past: the video system stores the most current video information for a period of time assessed as nominal for the facility. This could be a week, a month, or a year. The longer the duration, the more memory is required. Video streams are very data intensive, building automation systems are not as their messages are typically very short. Requiring logging of all network traffic for a year or more can be accomplished fairly easily with the low cost of hard disk drives. This archived information can be extremely valuable in the event a breach has occurred to help track, assess, and mitigate – something the legal team or internal audit team will be keen to ensure is available.

Real-time monitoring could be an inherent part of the control system for more advanced scenarios. Just like monitoring temperatures for out of range, monitor network traffic and origination sources for anomalies. However, the ability of any system to self-monitor relies on the design of the infrastructure and the components as well as tools such as protocol analyzers that become inherent to the system.

This is only recommended for facilities that have the IT staff to setup and manage such tools. Certain facility types will have strict requirements for monitoring their networks, such as military installations, bio-medical facilities, certain government facilities, and other high-risk environments. IT compliance measures must be implemented in these scenarios and this is a task for the IT professionals, not the OT staff, however, the designer and OT staff need to be aware of these requirements and factor that into the products and software specified for the project.

Facility Cybersecurity Assessment

Decision Matrix by Organization Risk and Type

A simple evaluation tool useful for assessing a project's cybersecurity requirements is to look at the facility type versus its risk or threat potential. Using a simple matrix such as the following can give the designer a simple starting point. Assessing facility risk is a critical piece of the design process as well. A simple matrix can help with the process. Using the following table, the project designer provides the basic assessment requirements for the type of facility. This should be done with strong input and coordination with the owner and other relevant stakeholders. For context, an office building with leased space tenants will have a significantly different risk profile than laboratory or a school. The first step is to identify the assets at risk such as critical equipment that, if attacked, might harm occupants, or information about the facility that, if obtained, may significantly impact business operations. The table below is a starting point for such an evaluation:

Tier	Function	Security Level	Cyber Security Risk
Enterprise Tier			Outside Network Threat - High Internal Network Threat - Medium Physical Intrusion Threat - Low
	Building Management System - Front End	System	
	Back Servers	System	
	Firewall/VPN Access	System	
Campus Tier			Outside Network Threat - Medium Internal Network Threat - Low Physical Intrusion Threat - High
	Building Automation System	System	
	Outdoor Lighting	System	
	Irrigation Control	System	
Building Tier			Outside Network Threat - Low Internal Network Threat - High Physical Intrusion Threat - Medium
	HVAC	System	
	Lighting	System	
	Security	System	
Equipment Tier			Outside Network Threat - Low Internal Network Threat - High Physical Intrusion Threat - Low
	Air Handler	Equipment	
	Lighting Panel	Equipment	

	Fire Panel	Equipment	
Devices Tier			Outside Network Threat - Low Internal Network Threat - Medium Physical Intrusion Threat - Low
	Thermostat	Embedded Device	
	Lighting Controller	Embedded Device	
	Energy Sub Meter	Embedded Device	
Source (used with permission):	© 2023 Ron Bernstein, RBCG Consulting www.rb-cg.com		

Cybersecurity Policies

All facilities require some set of cybersecurity policies be put in place to ensure continuous operation, minimize disruptions, and mitigate risk. The strength of these policies is closely related to the "intensity" of the measures required for the facility and the resources available to enforce them. Part of the risk assessment and cybersecurity planning is engaging with all stakeholders to ensure all requirements, constraints, and issues are addressed. Policy development and enforcement is often assigned to both the human resources department and the legal department. Having an unmatched set of policies with the level of enforcement can result in severely negative implications over time. Right-sizing the plan is crucial. Reviewing and revising the plan over time is also critical.

General BAS Cybersecurity Considerations

There are several issues to address that don't fall under any of the 4 Tiers. Addressing these issues in the project specification can help reduce risk and provide a mitigation plan in the event an event does occur.

Consider requiring real-time monitoring of all incoming IP network traffic attempting to access any BAS equipment. Log this access request as this may be helpful in tracing and preventing further damage if an event does occur. It can also be useful in working with IT security experts and authorities in tracking the extent and depth of the attack.

Requiring that all BAS controllers have full fail-safe programming as part of their applications is an advanced requirement but may be required in certain applications. This relates to attempting to stop a bad actor from modifying the control system or any equipment such that harm or disruption would come to occupants, the facility, or the equipment. Cybersecurity practices should be put in place to prevent potential sensitive data from being accessed.

Isolating the BAS device control network from any other network may be a valid solution to avoid attacks. In this scenario, as mentioned earlier, the BAS network and the site LAN are not connected. There are options to allow an intermediary gateway to bridge the two networks and only allow very specific data traffic to flow between them. Sometimes this is referred to as an "air-gapped system" or use of a "data diode" allowing only one-way flow of information.

Integration and Oversight

Some final thoughts: a good cybersecurity plan will include a basic process for ensuring compliance to the cybersecurity requirements. Define the stakeholders and their roles and responsibilities:

- IT and OT Roles Security ownership and validation
- Compliance Responsibilities
- Reporting a breach – how and who should get notified
- Ongoing system validation and compliance testing
- Hardness testing of supplier and contractor submitted solutions
- System updates, patches, and upgrades
- Human Resource onboarding and offboarding procedures for user credentials
- Emergency response team's action plan in the event of an attack or breach
- Legal contractors, ownership, liability oversight for compliance of contractors and vendors

Additional Tips For Improving Facility Cybersecurity–A Legal Perspective:

The following tips are compiled from legal contracts, policies, and procedures implemented by legal counsel to owners with moderate to advanced IT and OT cybersecurity risks. By implementing these procedures, owners have a more defensible position when working with contractors, clients, and customers.

- Require strong passwords, which must be changed at least every three months
- Make sure employees know not to share or post passwords.
- Train employees regularly on good cyber hygiene practices
- Review data backup frequency. Make sure critical data is backed up more frequently and all data is backed up offsite. Evaluate frequency based on ransomware lockup's effect; i.e., how many hours/days of data could you lose and still function?
- Follow your policy for retention and disposal of all sensitive information.
- Install software/firmware security patches as soon as possible.
- Encrypt highly sensitive data in storage whenever possible.
- Segregate sensitive data to reduce cross-over access by an intruder
- Implement IP address restrictions
- Disable/close unused ports on wireless routers
- Employ two-factor authentication (password and additional private information).
- Have an outside firm conduct regular risk analysis/risk assessment tests.

Source: Jason Bernstein, Cybersecurity Attorney at Barnes & Thornburg LLP – used with permission

Towering Innovation: Highly Efficient from the Ground Up

By Adrianne Mitani, P.Eng., Member ASHRAE; Greg Snaith, P.Eng.

MAINTENANCE & OPERATION

The mechanical systems of the building were designed to facilitate smooth operation, reliability, and low maintenance. The geothermal system allows for high efficiency operation, but without the added maintenance of an open cooling tower's water treatment requirements. While the water temperatures entering and leaving the geothermal field in summer and winter have to be monitored year after year, the maintenance of the building is not much different than for typical systems that reject heat to the outdoors. The property manager required education, as the system is fundamentally different than what they may have been used to when managing previous buildings. This included highlighting the importance of monitoring the geothermal temperatures and taking corrective action early if an imbalance is detected. Since the annual building load on the geothermal field is slightly heating dominant, the building's gas-fired boilers can be used to trim a greater amount of heating load to bring the geothermal field back into balance.

Mechanical equipment has been centrally located (as much as possible) in the penthouse, P5 mechanical room, and water entry room. Each hybrid unit in the residential suites has its major equipment components – including the compressor, fan, energy recovery ventilator system, and control valve – located on a removable chassis. The flexibility provided by this chassis results in minimal downtime for the tenant.

The major equipment located in the mechanical rooms is controlled and monitored by a central BAS. This optimizes the operations of the heating plant by centralizing the controls, reducing communication delays, and improving troubleshooting.

Systems were designed with redundancy for continued operation during routine maintenance and equipment failure. The boilers are sized for the full heating load of the building, should the geothermal system experience downtime. Three boilers and one central chiller and the hybrid heat pumps provide N+1 redundancy for heating, and the system pumps are in a duplex parallel arrangement that allows for one pump to continue running if the other fails or requires maintenance. The central heat pump's modular style also allows for

some equipment redundancy, and additional compressors in each suite heat pump allow for some cooling redundancy. A bypass was added around the waste water heat recovery system's waste water tank, should it require cleaning or maintenance. In the event of a power outage, the building also has a generator for systems on emergency power. The building was also designed to account for climate change. We collaborated with the structural engineer to make sure that the roof design would be strong enough to hold fluid coolers, which can be installed in the future to reject heat from the geothermal field if it is too hot.

COST EFFECTIVENESS

All design solutions proposed by the team were analyzed in terms of energy and cost savings. The decision to incorporate a geothermal heat pump system with sanitary energy recovery was a long-term, forward-thinking investment on the part of the client. Because 70 Gloucester is located in Ottawa's downtown core, this constrained footprint, in addition to CMHC funding, made the design decision to use a vertical geothermal system financially viable. After reviewing data surrounding the capital cost associated with this system with the operations team, the system was designed to prioritize a payback over years of operation to reduce carbon and overall energy usage. Compared to a standard OBC-compliant building utilizing the *NECB 2015* path of SB-10, 500,117 kWh of electrical energy was saved through the design of 70 Gloucester, with a peak reduction of 820 kW. The amount of natural gas saved through the implementation of the final design totaled 5,793 m^3 (204,578 ft^3). The final mechanical construction cost of 70 Gloucester was \$28.28/ft^2 (\$304.40/m^2).

ENVIRONMENTAL IMPACT

Due to the project's ambitious energy and greenhouse gas reduction goals, energy efficiency was critical in both the initial design and for the long-term operations of the building. The building was primarily modeled against a traditional natural gas *NECB 2015* reference building. Although this is an atypical approach, it is representative of how a project of this type would been designed in the absence of the high energy efficiency goals. For the purposes of demonstrating compliance with OBC 2017, additional analysis was conducted following the *NECB 2015* approach. Both energy analyses were conducted using *eQuest v3.65* energy modeling software.

In multiunit residential facilities of this size, the most significant overall consumption of energy is associated with space heating, space cooling and HVAC fan energy. Targeting these systems resulted in the greatest possible reduction in energy consumption. 70 Gloucester achieved 13.2%energy savings when compared to the OBC 2017 (*NECB 2015*). Compared to a standard OBC-compliant building, 500,117 kWh of electrical energy was saved through the mechanical design of 70 Gloucester, with a peak reduction of 820 kW. The amount of natural gas saved through the implementation of the final design totaled 5,793 m^3 (204,578 ft^3). The primary energy saving design features include hybrid heat pumps, which provide local heating and cooling, and the central ground-source heat pump plant. With proper care and maintenance, a geothermal energy field can be used indefinitely to provide a significant amount of heating and cooling over time.

Another energy saving design feature is the wastewater heat recovery system. This continual source of heat is directed to the domestic hot water system to provide preheated water to the penthouse domestic hot water system. As a result, a reduction in the heat required by the domestic hot water heaters is essentially “built in” to the design of 70 Gloucester.

In addition, natural daylight is supplemented by efficient LED fixtures, which are controlled by local occupancy sensors to further reduce energy consumption. Exterior lights are controlled by photocell and timeclock.

The final design of the project resulted in a 12.2% reduction in greenhouse gas (GHG) emissions (an equivalent to savings of ~36,000 $kgCO_2$/year) when compared to the OBC 2017 (*NECB 2015*). The building successfully met the requirements for CMHC funding.

Modernizing the Classic: Energy Efficiency Showcased

By Tracy Steward, Member ASHRAE; Tom Nicolas, P.E., Member ASHRAE; Jonathan Rogers, P.E., Member ASHRAE

Operation and Maintenance

The geothermal HVAC system is an exceptionally well-performing system regarding energy use while also reducing operation and maintenance costs. This system eliminates the use of cooling towers, chillers, and gas-fired boilers, which require extensive maintenance, water treatment, and service contracts. To provide synergy with ease of equipment maintenance and space acoustics related to HVAC noise, the units are floor mounted in distributed mechanical rooms separated by acoustical batt insulation in the walls. In the event of a repair, there are multiple service representatives in the area, and the project avoided the use of proprietary equipment. CMTA worked closely with the BAS contractor to simplify and optimize the building's controls to achieve the greatest performance. CMTA worked beyond the design and construction phases in this building to ensure systems functioned as efficiently as possible and worked through operation and maintenance issues. As a result, the new office building showcases the maintainability of a zero energy WELL Gold certified building.

Cost Effectiveness

The Well Project Administration carefully documented the cost of targeted WELL credits and as a consulting firm is able to demonstrate the cost of WELL credits to our clients who are pursuing WELL strategies in high-performance buildings.

The company leveraged the 10% geothermal tax credit, 30% solar tax credit, and EPact tax deductions. Leveraging the tax savings and advanced depreciation made energy efficient design an obvious choice for the building.