senseon®
SECURE ACCESS

HOSPITAL SECURITY STRATEGIC RISK ASSESSMENT: A TIERED APPROACH

A Tiered Approach to Hospital Strategic Risk Assessment

Inroduction

Hospital security professionals are facing uncharted waters.

While the entire healthcare industry is becoming more complex, hospital security is being transformed by increased cybersecurity attacks, new physical security challenges, and rising workplace violence[1].

But the real issue isn't just a rise in security challenges — the biggest problem is that *individual threats themselves have evolved*.

In days past, a security threat could be easily classified under singular categories like physical, electronic, local, or remote. But today's challenges are blending and intersecting — meaning healthcare security professionals are now dealing with ***multi-dimensional threats***. This is especially true in the world of physical security.

[1] Kaiser Health News

This new class of threats requires strategies that are multi-dimensional themselves and take a new perspective on physical hospital security.

Based on our 40 years' experience with physical security, we suggest a **tiered approach** that looks at risk from the viewpoint of the entire hospital but also takes a more granular approach. This perspective also addresses physical security at the floor and room levels, allowing you to incorporate solutions and technologies at each tier that fit that level of security concerns while at the same time, aligning with your high-level security goals.

In today's layered security environment, this approach pivots on access control as the primary security infrastructure needed for any hospital.

Hospital security leaders should consider this approach if they want to stay prepared for the challenges to come and protect their organizations from the inevitable potential losses.

> Hospitals are increasing spending on security — 56% are upgrading systems and staff
>
> ~HFM Magazine

The Problem: Hospital Threats Are Becoming More Complex

Look at any recent hospital security challenge and you'll see that it now crosses into multiple dimensions of security threats.

Opioid Theft

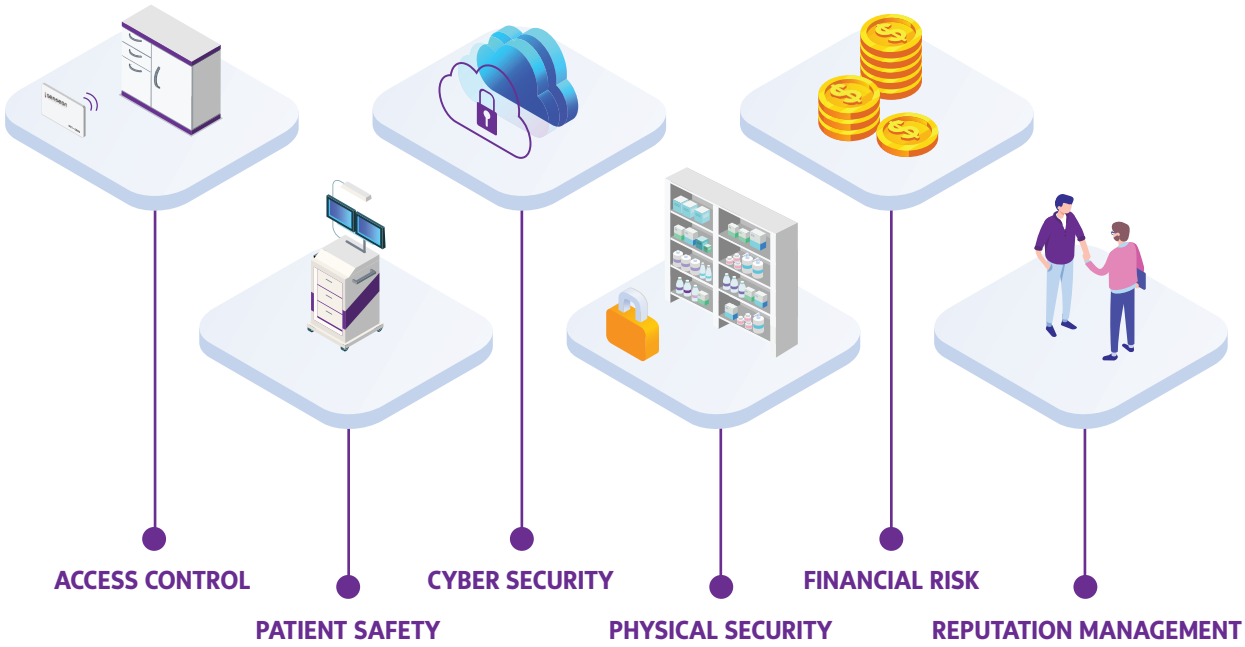
In the past, drug theft was purely a question of physical security. Today though, things have changed.

Just look at recent reports of clinicians illegally obtaining controlled substances. They now involve theft but also accessing automated electronic dispensing cabinets in medication rooms on patient floors. But it doesn't stop there. In the case of Kelsey Mulvey who has been accused of stealing drugs from Pyxis machines, 81 cancer patients failed to receive their pain medications[2] — a case where access control and patient safety intersect.

Stolen Laptops

Laptop theft is far from uncommon, but what used to represent the loss of a few hundred dollars in equipment is now more complex.

Look at the case of Advocate Health Care. In 2017, the hospital network earned the title of paying HHS the largest settlement ever by a single entity. They were assessed $5.5 million for potential violations of federal patient privacy laws that covered three, 2013 breaches, and compromised the patient data of 4 million people. Two of the incidents involved stolen employee laptops, a crime that not only resulted in lost equipment, but also financial risk for the hospital, cybersecurity risk, and damage to reputation[3].



[2] Medscape
[3] Modern Healthcare

Patient Safety

Today, patient safety is more than just posting guards at hospital doors.

Thanks to the double-sided nature of advances in medical technology, hackers can now worm their way into hospital systems and directly impact patient safety.

One of the most famous cases involved the remote hijacking of a drug infusion pump, but pacemakers, MRI systems, and even heart rate monitors carry similar risks, connecting the worlds of cybersecurity and patient physical safety[4].

The big takeaway? Yesterday's siloed, one-dimensional approach isn't enough. Most threats that hospitals face are now multi-dimensional.

A tiered approach to strategic risk management that segments the hospital into rooms, floors and whole facility/system allows security leaders to break the hospital into manageable physical tiers and address security threats from the simultaneous perspectives of cybersecurity, access control, and patient safety.

The Opportunity

The upside is that hospital leaders are responding in the best way possible.

A survey conducted as a collaboration between the American Society for Health Care Engineering (ASHE) and the International Association for Healthcare Security & Safety (IAHSS) surveyed 315 hospitals across the U.S., asking 32 questions about budgeting for security departments and technologies used.

The survey found that hospitals are increasing spending on security. Of those who are increasing budgets, 56% said they're upgrading systems and staff, and 50% said they're responding to risk levels. That trend is expected to continue[5].

[4] Alpine Security
[5] Healthcare Facilities Management Magazine

What are the benefits of a tiered approach?

A tiered approach isn't just a smart response to an increasingly complex security environment. It moves you closer to a security posture that aligns with the hospital of the future but also opens the door to additional benefits.

Better Strategic Alignment

Protecting a hospital is essentially protecting a small city of highly vulnerable citizens that's functioning 24/7. It requires layers of security and strategies that align with that reality. As challenges become more complex, strategies that overtly address those needs will become critical.

Accurate Asset Classification

As we mentioned in the laptop example, assets are no longer one-dimensional. A printer shared across one floor is now a potential source of a HIPAA violation if patient records are left sitting unattended, but also an endpoint that provides access to the rest of the hospital network. A tiered approach allows you to look at assets from multiple dimensions and more accurately classify its vulnerabilities to threats.

Improved Cost-Benefit Analysis

Investment in security technology now has more complex implications. For example, the cost-benefit analysis of an access control system now intersects with the potential risk around drug theft from a medicine cabinet in a patient room but also the risk of financial loss from HIPAA fines if a laptop is stolen from a cabinet. The total cost of ownership question is no longer straightforward and should be reconsidered in a modern healthcare security environment.

> "Hospital leaders will need to start considering new dimensions when conducting cost-benefit analysis of security solutions. Threats are now multi-faceted and one solution can easily be providing benefit on two, three, or more fronts simultaneously."

Enhanced Risk Management Results

A tiered perspective allows security leaders to make better choices around risk management. Healthcare security solutions are just as complex as the challenges, and evaluating and selecting vendor partnerships that align with your needs can be a daunting task.

Having a concrete perspective on your security needs will allow you to select solutions and services that get you to your risk management goals.

A tiered approach is also customizable to a hospital's unique needs, allowing you to respond to evolving security challenges faster and more efficiently.

A Tiered Approach to the Strategic Risk Assessment Process

Before we address the tiers, let's review the strategic risk assessment process.

For hospitals, physical risk management includes security, insurance, legal issues and of course, health and safety. Risk management is founded on the risk assessment process where risks are continually monitored and addressed. The five steps involved include[6]

- Asset Identification
- Security Inventory
    - Policies and procedures
    - Physical security
    - Security personnel
- Threat Assessment
    - Crime analysis
- Vulnerability Assessment
- Risk Assessment
    - Cost-benefit analysis
    - Report and recommendations

While this process is traditionally applied at the hospital level, it can also be shifted to a more granular approach and condensed down to the floor and room level as well.

[6] Karim H. Vellani

Hospital Tier

Risk assessment at the hospital level is founded on a properly designed and built environment. It involves healthcare-associated infections, patient falls, access control posture, network security, medication errors, and general security risks. It includes intangibles like reputation and branding and external concerns like cloud security and off-site storage.

Considerations will be made around facility entries, network protections, and vulnerabilities to potential terror threats. Asset questions will be broad, security inventory extensive, and threats, vulnerabilities, and risks will need to be addressed at a holistic level[7].

Floor Tier

Risk assessment at this mid-level tier will vary depending on the departments and function of each floor.

Asset identification will involve doors, informational assets like physical medical records (if housed across a particular floor), patients, supplies, and pharmaceuticals, while security inventory will involve security cameras, badges, security personnel, and network endpoints.

Vulnerabilities at the floor level can include shared printers and imaging equipment, location of nurse stations, and floor-specific access points.

[7] Agency for Healthcare Research and Quality

Room Tier

Room risk assessment will vary based on room function, department, and potentially even location.

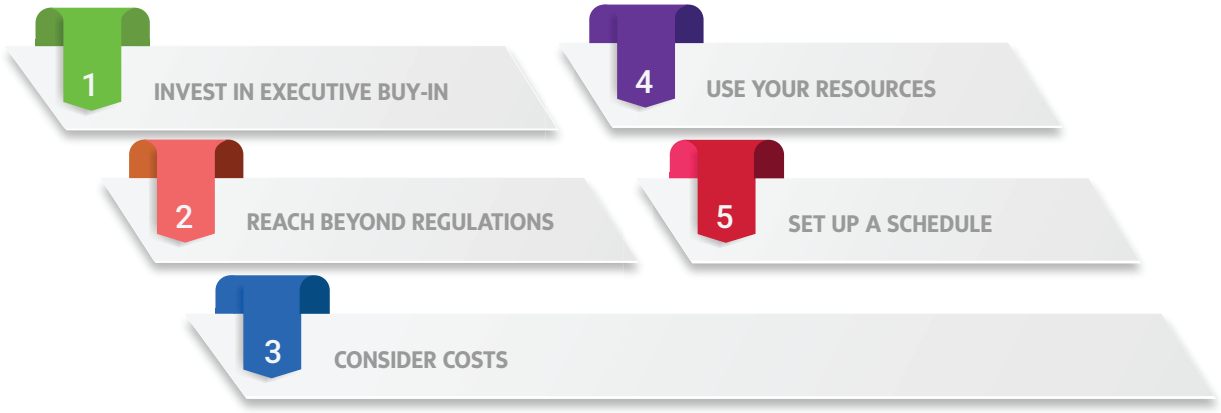
Asset identification will address what personnel (clinical and non) that access the room, the devices and supplies that are used in the room, cabinets, drawers, and proper classification of critical and non-critical assets.

Security Inventory will include furniture-level access control equipment, security personnel, location-specific security management (i.e, the ED since it tends to exhibit higher levels of violence).

Threats and vulnerabilities at the room level can include drug diverters, and cabinets and drawers, as well as medical devices.

Risk Assessment Best Practices

While a tiered approach will allow you to adjust to modern security threats, make sure you're considering these practices when establishing your new risk assessment program.



Invest in executive buy-in.

Hospital security requires collaboration, and you're going to need support from IT staff, clinicians, marketing, and potentially even patient community representatives.

Gaining input and assistance at that level will require allies in leadership positions across the organization. Since security impacts the entire organization (a breach, for example, can cause hospitals to spend 64% more on advertising)[8] and budgets are expanding, now is a good time to make a move.

Reach beyond regulations.

While regulations like HIPAA and OSHA standards can provide a strong incentive to conduct risk assessments, they shouldn't be your primary drivers. Move past a reactive approach and develop standards that align with your organizations' mission and values, making sure to prioritize improved outcomes and providing a premium patient experience.

Consider Costs.

A tiered approach to risk management will include rethinking many of your security investments. When assessing purchasing decisions, make sure you're considering both ROI and total cost of ownership.

Use your resources.

Hospital risk assessment is complex, but thankfully, multiple organizations offer toolkits and other resources to help you build out your risk assessment strategy. For example, AHRQ offers this Health Care Facility Design Safety Risk Assessment Toolkit.

Set Up a Schedule.

Risk assessment shouldn't be a one-and-done job. Use your past experiences and risk profile to determine how often assessments should be conducted.

Most importantly, when developing your risk assessment strategies, make sure you're working with trusted security partners who understand your perspective and who can ensure your peace of mind through specialization at both the asset and industry level.

[8] AJMC

Resources

[1] Escalating Workplace Violence Rocks Hospitals

https://khn.org/news/escalating-workplace-violence-rocks-hospitals/

[2] Nurse Accused of Stealing Opioids, Replacing Them With Tap Water

https://www.medscape.com/viewarticle/914546

[3] The frightening new frontier for hackers: Medical records

https://www.modernhealthcare.com/article/20170410/NEWS/170419987/the-frightening-new-frontier-for-hackers-medical-records

[4] Most Dangerous Hacked Medical Devices

https://www.alpinesecurity.com/blog/most-dangerous-hacked-medical-devices

[5] 2018 Hospital Security Survey

https://www.hfmmagazine.com/articles/3519-hospital-security-survey

[6] Strategic Security Management: Risk Assessments in the Environment of Care (Karim H. Vellani)

https://pdfs.semanticscholar.org/24e5/df5b0f8067f59139108ee8a5ba744feb35d0.pdf

[7] Health Care Facility Design Safety Risk Assessment Toolkit

https://www.ahrq.gov/patient-safety/settings/hospital/resource/safety-assess.html

[8] Understanding the Relationship Between Data Breaches and Hospital Advertising Expenditures

https://www.ajmc.com/journals/issue/2019/2019-vol25-n1/understanding-the-relationship-between-data-breaches-and-hospital-advertising-expenditures?p=1

senseon®
SECURE ACCESS

888.337.4096
senseoninfo@accuride.com

www.senseonsecure.com