Outline for Session

- What is the responsibility of owners and managers relating to cyber security?
- How do you ensure that your current building systems are not susceptible to hacking?
- What steps can you take to minimize the impact of a cyber attack at your facility or portfolio?

BACKGROUND ON CHANGING ROLES

- “Our” business collectively has **materially** changed over the past 20 years since the 1993 bombing of the World Trade Center and will continue to change

- Many of us can recall times before that incident, it was a simple business model (budgets, operations, tenant relations, returns, protect the assets value, etc.) – KEEP THE LIGHTS ON

- Fast forward to today, concerns range from:

  - Maintaining Basic operations, to
  - Pandemic issues, to
  - Increase in natural disasters, to
  - Being advised of Infrastructure issues/ deferred maintenance of life line services, to
  - Warnings about Terrorists or wannabe’s, to
  - Gun violence on the rise, to
  - Drones, what does it mean, to
  - Cyber issues within our facilities or at home where our stuff and that of clients could be compromised.

- ***Risk*** has become and will continue to be a major issue for each of us

Possible scenario

- Tenant contact asks to stop by your office this afternoon.
- When individual arrives he/she is joined by two people who identify themselves as being from the **cyber response team of the FBI.**
- They advise that the tenant's systems have been hacked dating back nine (9) months and want to review all records and confirm that the building systems weren't used to create incident.
- They will need access to all records and documents pertaining to your firms cyber protection programs. They expect to be onsite for the next three (3) weeks – Starting now.
- What exists to support your defense?

Cyber review – Landlord's potential exposure

- Areas of concern – Landlord's perspective
  - Increased threats and attacks on mechanical, security and communication equipment and systems require due diligence to identify potential risks:
    - Point of Entry rooms – access control, security and record keeping
    - Fiber backbone – responsibility and protection
    - Base building systems and service contracts
      - Care of systems, updates/patches, changes to passwords when staff occurs
      - Access controls – cyber hygiene, reporting when hacks occur, etc.
  - Systems and services overseen and directed by Landlord and by outsourced property management firms
  - Allocation of risk and responsibilities among Landlords, property manager and other building vendors

Suggested Process – Team's or IREM members

- Four (4) Steps
  - #1 - Develop knowledge of what exists today
    - Complete an inventory of Computers (mgt office, engineering, security, etc.), devices, systems, wi-fi, etc. where team members can access the web or vice versa where others can monitor systems. – **Document** serial numbers, IP addresses, etc.
    - Conduct tour of property, meetings w staff to discuss inventory. Anything missing? - **Document**
    - Understand and discuss how tenants interact w property team to schedule services (i.e. HVAC, room reservations, etc. – **Document**
    - Review of Point of Entry rooms for:
      - Process and protocols – does it comply with firms corporate guidelines, is access limited to approved groups. What is process to maintain records. **Document**
      - Security of room – access control vs cylinder locks, CCTV's, role of fiber mgr
      - Potential investment for segregating services – Costly!
    - Identify all Service Agreements in place or may be required to protect cyber operations
    - Examine what training is completed to confirm ALL staff follow good cyber hygiene practices and when changes occur – new hires, replacements to include service technicians. **Document**
    - Educate ownership as to effort and findings, discuss process and desire to engage professionals

Suggested Process – Team's or IREM members

#2 – Review existing service agreements (SA) and meet with providers

- For example:
  - BMS/BAS systems – who owns the computer, what are responsibilities for patches, etc.
  - Fiber backbone – what is included, roles and duties, periodic reports, audits, etc.
  - Local/national resources used to provide patches – does PM corporate provide support or does agreement exist with local firm to provide support – what is included and not?
- Service agreements may or may not identify systems which provide access to building systems. (i.e. Computers purchased for BMS/BAS systems may not be included) – patches, passwords, etc. **Responsibility, Frequency and documentation**

#3 – Engage local, regional or national resources to review work product for:

- Discuss results of findings – include all key team members in discussion
- Have outside firm conduct non-destructive testing of systems to confirm findings and identify potential risks, correct with new procedures, patches or newer systems
- Confirm what work arounds may need to be required to run systems in independent mode vs losing access to operations
- **Document** all discussions and findings

Suggested Process – Team's or IREM members

#4 –Change operations to account for:

- As service agreements come up for renewal review each for:
  - Roles and responsibilities for system maintenance, change in personnel, frequency of password changes, what happens if contractor gets hacked?
- Encourage all staff to follow good cyber hygiene, create steps for new or replacing of individuals to confirm integrity.
- Periodically have outside firm test systems through non-destructive testing
- Include Sr leadership in discussions as to efforts and periodic updates.
- Monitor thru IREM, BOMA local and other sources for cyber threats or actions which may impact other groups (BOMA, RE-ISAC, NCRIC, FBI Cyber, etc.)

Summary and Conclusion

- What is the responsibility of owners and managers relating to cyber security?
  - Understand your buildings key features that support the internet
  - Make sure you have good cyber hygiene and is tied back to firms corporate programs. Don’t follow some program which you have used at other properties or inherited.
- How do you ensure that your current building systems are not susceptible to hacking?
  - Document any and all systems that have an IP address or systems you and others can tap into from outside the bldg.
  - Hire a qualified firm to run diagnostic testing to identify weaknesses and cure.
- What steps can you take to minimize the impact of a cyber attack at your facility or portfolio?
  - Confirm that fire walls and patches are current including PM, engineering office, BMS and other systems.