Burns & McDonnell
SINCE 1898

Engineering, Architecture, Construction, Environmental and Consulting Solutions

WEBINAR

Effective Security Planning and Integration

Presented By:

Burns & McDonnell Global Security Services

Presenters

Stephen A. Brown, CPP
Director, Global Security Services

Dale A. Braathen, CISSP
Cyber Security and Government & Defense Services

Robert "RJ" Hope, CPS, ABCP
Physical Security and Business Continuity

Burns & McDonnell

Kansas City, Missouri

- Architectural, Engineering, Construction, & Environmental Consulting Services Firm
- Founded in 1898
- 3,000+ Employee-Owned Company
- No. 50 – 2009 Fortune 100 Best Companies To Work For
- Ten Regional Offices Throughout The United States

World Headquarters

Today's Webinar Will Focus On Seven Key Areas

1. Assessing security since 9-11
2. Protection of your critical assets
3. Your response to suspicious activity and/or alarms
4. Your security policies, procedures, and training
5. Effective cyber security measures and data recovery
6. Adequate business continuity plans
7. Your risk from neighboring organizations

Since September 11, 2001

- $100,000,000's of dollars have been spent on access control, CCTV, and intrusion detection systems.
- Security systems no longer work as designed or have become outdated and causing vulnerabilities?
- Employees are lax and allow access into your facilities via piggybacking and tailgating.
- Have your cameras been repositioned and no longer monitor or record what you thought or need?
- Can you positively identify the people in your videos?

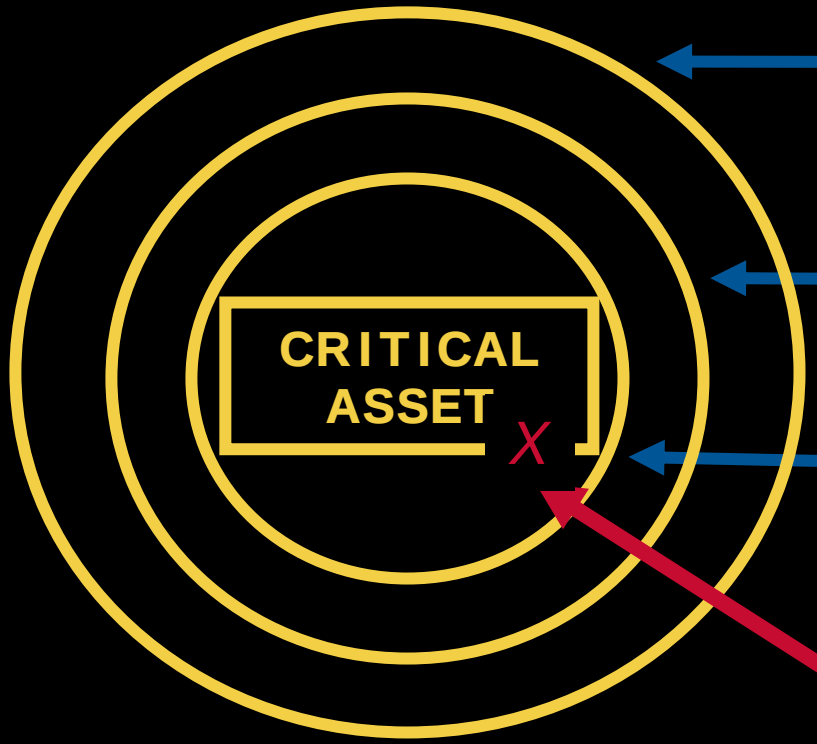
Since September 11, 2001

- Over the past eight years, have your security operations procedures kept up with trends and technology?
- Have unauthorized persons become common place in your facilities? What procedure do you follow?
- Layoffs and terminations are taking place or on the horizon for most companies.
- Workplace violence and active shooter incidents have increased in recent months.

Are you getting the same or better return on investment for your security system today you were getting five years ago?

But more importantly, are you as SAFE today as you think you are?

It all comes back to RESPONSE !



DETER

DETECT

DENY / DEFEND

RESPONSE

Concentric Layers of Security

- Soft Target vs. **HARD TARGET**
- Aggressors, contractors, vendors, former employees, even current employees are sizing you up.
- Are doors, gates, windows propped open?
- Do security officers take their break or make their rounds at the same time each shift?
- Who is becoming best friends with your security personnel, and why?

- It will amaze you how much outsiders know about your business.
- In some situations, aggressors know more about the everyday comings and goings of daily routines than management personnel.
- WHY? Because management becomes complacent and falls victim to the lack of security awareness training and staying on top of security initiatives.

Case In Point

- This type of scenario happens more than you know.
- It does not matter the type of business you are in, there can be compromises in your security at the very basic level and you not know it.
- So we go back to our very first statements:

- Since 9-11, considering the millions of dollars that have been spent on access control, video surveillance, and intrusion detection systems, are you getting the return on your investment and are you as safe today as you think you are?

Let's Look At Our Scenario

Deter: The company had a fence with locked gates.

Detect: The company had an alarm contact on the gate and a camera in place. So they thought!

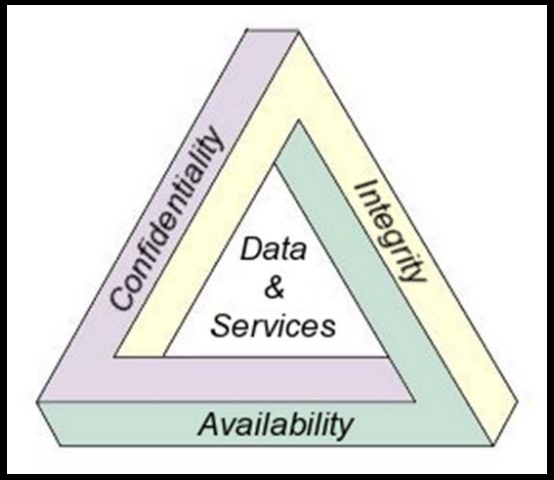
Delay/Defend: The company had security officers and an internal fenced cage for the chlorine.

Response: The company thought they had a response plan in place, but now they will wait 5 hours to formally respond.

Does This Type Scenario Sound Familiar?

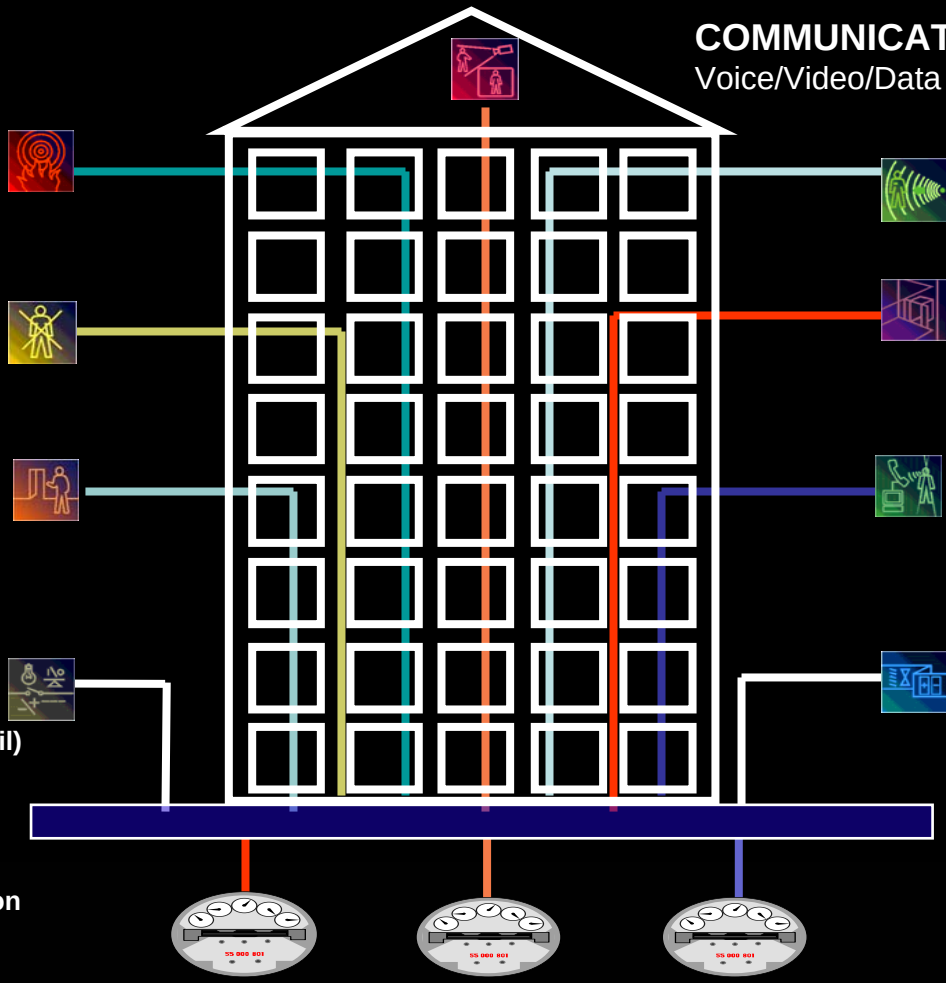
The cost of an *independent and thorough* assessment now, is far less than the cost incurred by not being prepared when an incident happens.

Cyber Security



- Cyber Security is an integral part of your business.
- Confidentiality ensures your secrets are maintained.
- Integrity provides assurance that your data has not been tampered with.
- Availability allows you to have your data when and where you need it.
- Security in-depth with multiple levels of protection is a best practice.

Cyber Security



COMMUNICATIONS
Voice/Video/Data

FIRE
Functionality checks
Detector service
Fire, Life, Safety

SECURITY
Doors/Cameras
PIR
Integration

ACCESS
Doors
Buildings
Occupancy
Feed Forward

ENERGY
Utility Monitoring (Elec/Water/Gas/Oil)
Tenant Building
Air/Water
Heat
Lighting
Back-up Generation

LIGHTING
Schedules
Occupancy Sensing

ELEVATORS
Breakdown
Maintenance
Traffic Performance

24/7 OPERATIONS
Breakdown
Plant Tuning
Conditioned Monitoring
Car Park Utilization

HVAC
AHU's, Boilers, Pumps, Fans
Energy, VAV's, IAQ

Case Study – Maroochy Water Services

Players

Employee: Vitek Boden

Contractor: Hunter Watertech

Product: SCADA Radio-Controlled Sewage Equipment

Client: Maroochy Shire Council

Scenario

- Boden leaves Watertech following a strained relationship and applies for position at the Maroochy Shire Council.
- Boden keeps a Watertech laptop with radio communicating equipment attached to it.
- The Maroochy Shire Council did not hire Boden.
- In retaliation, Boden drove around the area and on at least 46 occasions issued radio commands to the sewage equipment.

Scenario

- Boden's actions caused 800,000 liters of raw sewage to spill into local parks, rivers and onto the grounds of a nearby Hyatt Regency hotel.
- During an attack, Boden was apprehended as a result of a traffic stop. He was sentenced to 2 years in jail.
- Boden was also ordered to reimburse the Maroochy Shire Council for the massive cleanup.

Case Study Observations

- An employee of a Contractor was a trusted insider, never an employee.
- Appropriate employee separation procedures were not in place.
- Cyber security policies and procedures were non-existent or inadequate.
- A skilled insider with advanced knowledge disguised his actions.
- Security of radio communications equipment was very inadequate.

Lessons Learned

Improvements in the following areas are warranted in this case:

- Personnel surety and security
- Contractor supplied hardware & software
- Security awareness and training
- System lacked sufficient audit capability
- Contingency plans
- Formal incident response
- Cryptographic protection of communication and support of identification and authentication. (Possession of radio and computer alone should not have granted access)

Case Summary

- Defense-in-depth is a best practice
- Inside & outside attacks must be considered
- An individual with detailed knowledge of the system could potentially defeat controls

Cyber Security Considerations

- Risk Assessments / Information Security Auditing
- Disaster Recovery/Business Continuity Planning
- Regulatory Compliance: FISMA, HIPAA, SOX, GLBA, Privacy Act, HSPD-12
- Certification and Accreditation: DIACAP, NISPOM, NIST
- Develop Information Security Policies, Standards, and Procedures: ISO 17799/27002, DIACAP, NIST, COBIT
- Data Protection: VPN, Encryption, Authentication, Single Sign-On

The cost of an *independent and thorough* assessment now, is far less than the cost incurred by not being protected when a hacker breaches your critical cyber systems.

Crisis Management and Business Continuity

Hurricanes

Criminal Mischief

Chemical Release

Labor Strikes

Workplace Violence

H1N1

Terrorist Attack

Bomb Threats

Sabotage

Fires

Tornados

Civil Unrest

Floods

Business Continuity & Disaster Recovery Names

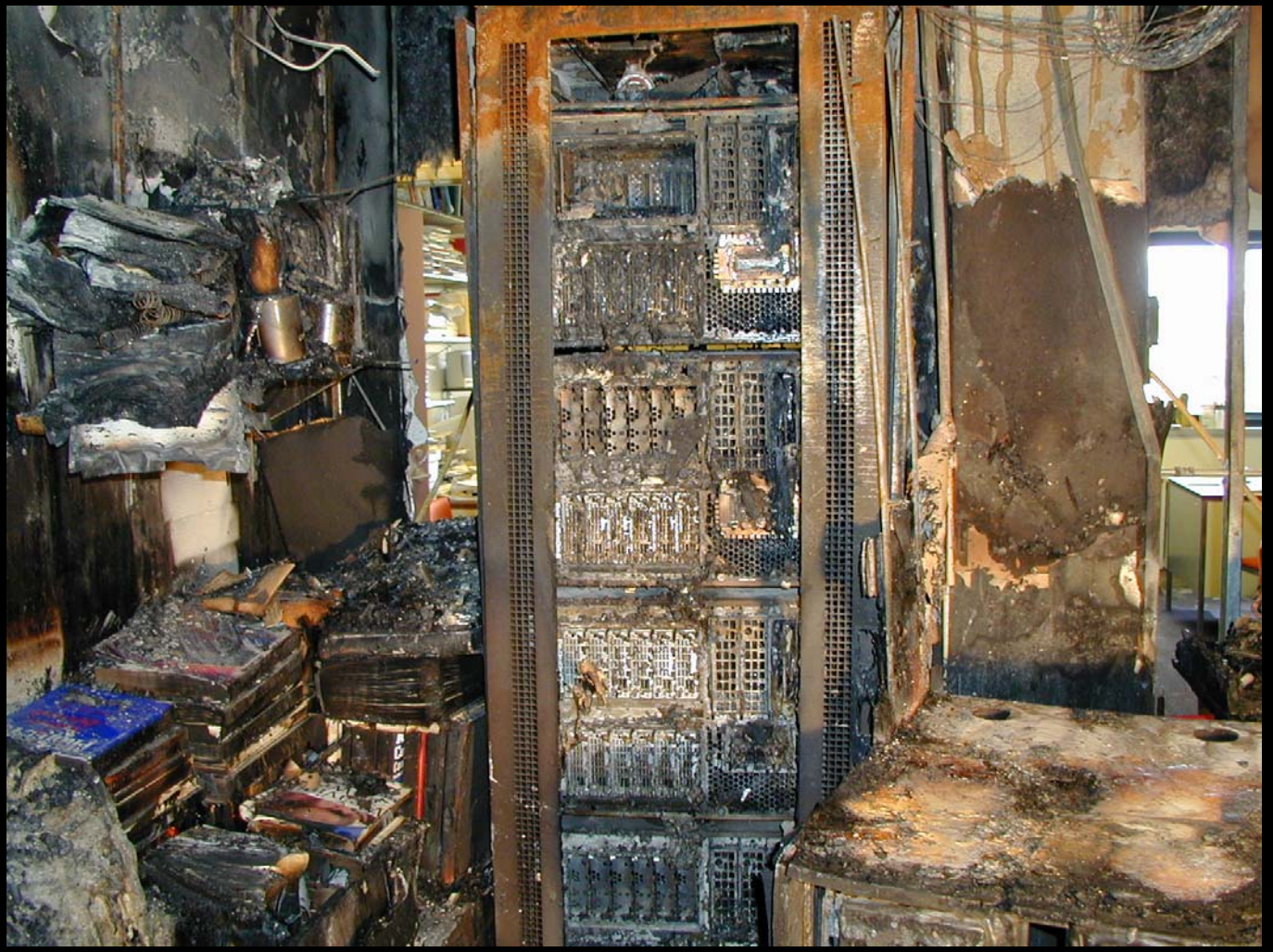
- Business Continuity & Disaster Recovery Plans
- Business Continuity Planning (BCP)
- Business Impact Analysis (BIA)
- Business Resumption Planning (BRP)
- Disaster Recovery Planning (DRP)
- Emergency Response Planning (ERP)

It doesn't matter what you call it.
It needs to be up to date and current!

This is not the time to begin developing your Crisis or Business Continuity Plans!

What about Data Center fires?

When could you be back up and running?



Are the Yellow Pages your go-to document when a crisis hits?

This building just became uninhabitable due to a minor accident.

It's time to move operations.

THREE
Misconceptions

1. "Hey, the risk is so small why worry about it?"
2. "You know, if something were to happen, we couldn't stop it so why bother?"
3. "How do you expect us to prepare for ***EVERYTHING***?"

Risk of Event = Financial Cost of Occurrence

How do you continue to produce your products, provide your services, invoice your customers, receive their payments, and meet your payroll if your primary place of business became **UNINHABITABLE?**

- When was the last time you thoroughly assessed and tested your business continuity plans?
- When was the last time you evaluated current threats and the risks of these threats to your business based on today's security environment?
- Have the manmade threats to your business changed in recent years?
- What are the risks to your business from these threats?
- How vulnerable are you to these risks?

Let’s look at a recent scenario where the failure to have adequate monitoring and response plans in place almost created a massive crisis.

Two teenagers dressed as Ninja's made their way to a 4th floor control room in this power plant.

Please pay close attention to the breaker under the red arrow.

As a prank, they began turning knobs, not realizing the damage they could create.

Keep in mind, they made it past the access control, CCTV, and intrusion detection systems completely undetected.

The breaker this Ninja skipped over would have shut down the plant and cause millions of dollars in damage to the equipment.

What about the effect on the local community from the extended power outage?

Let's consider neighboring businesses.

You should know what your neighbors do *and* how it could affect

YOU!

- Who are your neighbors and what do they do?
- If they had a major catastrophe would it affect you?
- When was the last time you sat down and discussed crisis management with your neighbors?
- When was the last time you sat down with local law enforcement and/or federal responders and discussed how a crisis might affect your business?
- Do you have this documented with plans in place?

Here's another recent scenario that put many businesses on notice that a crisis can come from anywhere.

Do you think the downtown businesses planned for such an event over three miles away?

- Successful businesses have good intentions.
- Successful security and crisis management plans include potential threats that may arise outside your property line.
- Do you have up to date security and crisis management initiatives in place to support you in the event your business neighbor has a crisis?

The cost of an
independent and thorough
assessment now,
is far less
than the cost incurred
by not being prepared
when a crisis arrives unannounced.

In Closing

- Our goal today was to create thought provoking questions to assist you in strengthening your security profile.
- Do you have up to date physical security procedures in place that take over when the phone call comes in the middle of the night?
- When you put your head on the pillow at night, are you certain your critical cyber systems are protected from hackers?

- Your business evolves everyday. Have your Business Continuity Plans evolved with it?
- Crisis situations arrive unannounced. Are your current plans and procedures ready and up to date?
- When was the last time you met with your neighboring businesses and discussed crisis and/or security action plans?

One more survey question before we end.

Now is the time to *thoroughly* assess your physical security response procedures, your cyber security procedures, and your crisis and business continuity plans.

The cost now will be far less than the cost incurred if you are unprepared and an incident happens.

Let's End Where We Began

- Everyone knows 9-11 changed the world.
- Collectively, $1,000,000's have been spent to install integrated security systems.
- Business continuity and crisis management plans were the buzz words shortly thereafter.
- Everyone, at one time or the other felt very good about their security posture.
- But, where are you today?
- Are you as **READY** as you think you are?

Our certified security professionals are ready to answer your

Questions

Stephen A. Brown, CPP
Director, Global Security Services
816.349.6754
sabrown@burnsmcd.com

Dale Braathen, CISSP
Project Manager
816.822.4317
dbraathen@burnsmcd.com

Robert "RJ" Hope, CPS, ABCP
Physical Security Analyst
816-333-9400 x5028
rjhope@burnsmcd.com