PHYSICAL SECURITY TECHNOLOGY

1

- The technology side of physical security is a slow moving glacier compared to the rest of technologies so it's not the most exciting subject. It is controversial because In the wrong hands it could be a horrendous spying tool, but in the hands of a security professional it offers the chance to make the world a safer place for all of us. IT is on the brink of becoming heavily involved in security technology
    - I am David Figge and I was asked to speak on the subject of the technical horizon of physical security because I work in a manner that bridges the gap between the two. I am both an owner and a founder of multiple companies
    - One company I own is a profit centered imbedded consulting and account management company which specializes in multi-disciplined technical sales. We design and sell physical security into education, healthcare, commercial and government)
    - One is a app development (evernote)
    - Explain the metaphor

- To fully speak on the subject of the where tech is going in physical security we have to understand understand it's history, where we are now and the pressures and players that drive this industry

TODAYS FOCUS

2

- Security has many elements, there is access control (badges, credentials), there is Video, There is alarm intrusion and guarding. There are also other forms of security such as CPTED (explain).
- The two that will effect you the most in the technology space (Access Control and Video). Those will be the ones that most likely their components will reside on your network.
- Lets begin by laying a foundation so that you truly have understand who the players are now and will be in the future and what the pressures that are driving innovation in physical security.
- This will allow us to not just hear about the new technology but also evaluate best practices on addressing it.

3

There are multiple players with slightly different focuses. Each one of them bring some form of value to the table and working as a team will truly be able to help limit the impact on your system and infrastructure.
IT (data and information)
Physical Security (people and safety)
Manufacturers
Integrators

Physical Security Tech- What Drives Innovation?

4

The term physical security conjures up a lot of images, but technology typically isn't the first thing that comes to mind. There is a reason for that.

1. I would love to say we are a pro-active…and we are a step ahead. We are not. At best we are reactive to the world around us we are often a step behind. A few years ago I was contemplating security and how to take down nations. Unfortunately I was able to come up with a way that would guarantee about a 95% success rate and take down an entire country for about a total of $3,000 and would only take a few days to accomplish. Is there tech that could prevent it? yes.…it would be cost prohibitive…but that's the rub cost vs. security.…proactive vs reactive. budget open up reactively..Technology costs money and security tech is often the last to get funded.

So when do we leap forward…Unofrtunately It's Columbine, It's the World Trade Center, It's 9-11, It's Sandy Hook, and in our local world It's a disgruntled employee, or a security breach, it's these types of incidents that really drive the technology in our industry…

AN INDUSTRY REVOLUTION

5

1. But with that said, Well we are on the brink of a real evolution in our industry
    1. We are smack in the middle of a shift of who and who is making decisions in the physical security space. In the past it was not complicated. Facilities was the main decision makers. It was their kingdom…it was their budgets…but that is quickly going way.
    2. The best companies are taking a team approach involving security personnel, technology personnel, and relying on multiple players to help make great technology decisions
    3. And the technology is…is…just starting to be driven by other factors outside of incidents..manufacturers are starting to make some real innovative moves (I'll talk about that later on in this discussion)

ACCESS CONTROL

6

- Let's start our discussion today at the door level…what is new in entry technology.
- Access control is anything that allow for the possibility of entry, audit, monitoring of a secured area or building
- To see where door security is going, we definitely need to see where it's been…
- One of the big advances was Skeleton Keys which were Very low security…but soon came master keys

-

ACCESS CONTROL

7

- Master keys and interchangeable cores—-a single key to rule them all…but there was no way to audit so along came ((click))
-

ACCESS CONTROL

8

- Electronic entry past (magstripe, dallas chip, barcode, pincode, and scramble pad)
-

ACCESS CONTROL

9

- So where are we right now….
- Predominately we have magstripe and proximity cards (both standard and iclass) and
- To date only about 5% of a buildings openings have access control tied to them.
- and just so you know about 74% of college campuses still are on magstripe
- Where is this technology about to go next

10

- Readers first then credentials

- On the reader side well..the smarts used to reside on a server…then it moved to appliances…now it is moving to the edge. So there is no formal front end system…just reader and browser based interfaces
- To be honest though the industry has been trying to move away from a traditional server environment to the edge for a while…but every time we push away from it, we find that we have to go back for one reason or another.

Let's discuss two of the latest technology as it pertains to access control

ACCESS CONTROL

11

On the credential side…we

- Ok…this one is obvious…On the horizon (NFC (smart phone)/RFID) (ASU pilot programs), Problems
- 1. Standardization (had to get special phones with a specific standard)
    - Problem 2. Battery…can't open without a charge
    - Lost phones
    - Still needed a pin code and often a physical key…that's the interesting part …those are almost always needed. I would liken it to always needing a 5.25 floppy disk drive and at least one vacuum tube in every computer you have.
- The next frontier in the access control and token side is Enhanced biometrics

ACCESS CONTROL

12

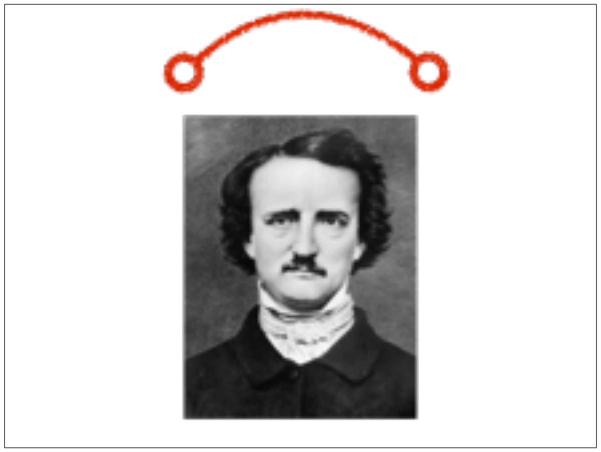
- Ok some of the cool stuff…
- Enhanced biometric readers

Here CSI stuff and stuff movies are made out of …

- I mentioned this beforeFingerprint is still in the game…but with heat signature
- facial recognition …still in it's infancy
- vein pattern
- retina/iris recognition…improved watch this (click) ….tell the bus story (didn't tell the parents)

Other things to watch for include:

- Sustainability and net zero. 2050 initiative. solar/static and other methods to power these readers..while we are on power…



13

- I want to quickly mention Power (POE)…POE is being used readily now both on lock power and reader power and even video power
    - I mention it because of The switches that are being sold to you by the integrators probably do not meet your standards (low bid)they might be being bought from merit time or … But they may also be in a closed system (just be aware). the shift to POE is going to play into the sustainability aspect of powering devices…sure, but if you have a standard you need to communicate that to the people involved with access control and video

-

14

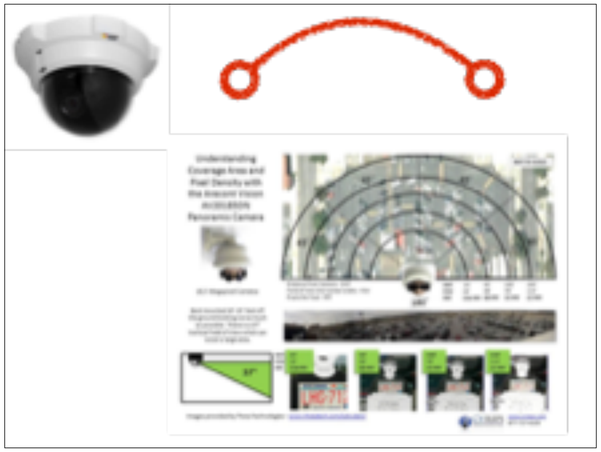
So What about CCTV/Video

Sources (IHS Report on CCTV trends), Security Systems News and my own opinions

Ok…first off how does this portion of our industry work?

1. We follow the porn industry when it comes to video technology (true)
2. We are bit slow to adopt and therefore slow to advance (many have just recently entered the megapixel world) hang nokia lumina from the ceiling
3. We do have an industry standard (sales people love to talk about it) and in real life it is awful (ONVIF)
4. Let’s look at the some cool stuff that can be done and where we are going let’s start with camera

-


Understanding Coverage Area and Pixel Density with the Arecont Vision
Panoramic Camera
LHG-71

15

1. We are just reaching the tipping point where Aanalog camera's on coax and now beginning their decline and IP Megapixel camera's are rising. In the old analog days we used guess work on where and what a camera could see "if you see it it sees you"
2. With IP and megapixel camera's you now know what you are going to be able to see. we use pixels per foot to describe the data (show and explain the picture above)
3. Just FYI Most of the industry is limited to 5mp for many reasons…but even with 5mp there can be times where there is a lot of video being transmitted across your network.There is a variable impact on your bandwidth. h.264 is only recording changes in the scene..But right now IP camera's are bad in low light. You want to see a spike in the network activity…just throw is a blowing tree…or a snowstorm…or just night..you need to test these camera's in your own environments to fully understand their impact. Of course there is closed systems if you prefer

-

16

- And then there is audio? Sound …recording conversations…that's not in the news huh?
- What you are looking at here are audio recording devices…
- Many video IP camera's have the capability already to record audio (explain the slide). But many companies have not utilized this feature…boy that is rapidly changing and Utah will be one of the earliest adopters of that trend for sure because our laws (let me explain). How that will impact storage will be very important to your world.

-

Stored in the cloud
No ongoing costs

17

- What about storage?

- We had VCR's……then DVR's (proprietary boxed computer..expensive) ..then hybrids……we are now reaching a and NVR's that not only accept ip cameras with encoders for legacy analog cameras. NVR's of these are finally able to be installed on a virtual machines which will make life better for everyone. The interface is all the security professional is typically worried about But you need to be thinking about
- who owns/maintains the server
- How much space and resources really need to be allocated (I've seen 700tb server farms dedicated to video)
- Bandwidth

-

One-click setup with Axis cameras

18

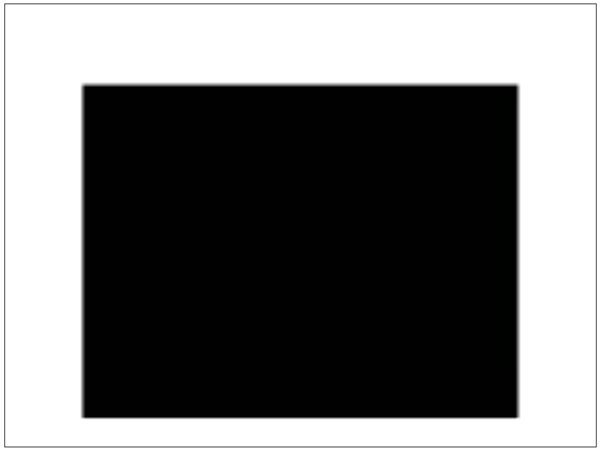
- Cloud based video …VSAAS (video surveillance as a service)? Well obviously the Cloud is coming…right now it's more like fog though….but it has many hurdles to overcome..the manufacturers are being aggressive about solving those issues..what are some of the problems?
  - Bandwidth 30fps..so some require a NAS device be included for each camera (a bit self defeating)
  - Who manages the video…how secure is it where it is residing (integrators)
  - firewalls
  - price…still have to buy a camera and install it…it's just the front end cost

-

19

OK some of the cool spy stuff

- Thermal imaging is an awesome new too
- high radiation site (story)…animals…people…terrorist



20

And Analytics…why its important “20 minutes of monitoring and the person is below acceptable standards"

- What can we do with analytic currently ((click))

21

- First came Virtual fences and lines…now ((discuss the slide))
- Where the industry is is pretty cool…we have some real innovation taking place.But where we are about to go…well…let's make some predictions.

PREDICTIONS AS TO WHAT IS NEXT

22

So what's next

1. Prediction 1: The cloud (on the coast no longer called the cloud). Access control will eventually move from an onsite servers hosting software to true SASS. We are going to see more and more manufacturers moving data into the cloud and the integration between HR and access control will be tighter and tighter. How this plays out will be interesting to watch, There will be many turf battles but eventually I cannot foresee a reason why when an employee is on-boarded there won't be a one system single input system

Access Control

23

The future predictions of Access Control are less about readers and front end and more about utilization

Social Buildings will soon come into play (and already are in infancy) . Like a key and lock, for the foreseeable future you will always need a human guard just for safety. but the coordination between systems will be huge and will take buildings to a new level. Smart Sensor technology and interaction between devices you could
invite someone to your building
they receive an access token
They are welcomed to the building by an automated device a map appears on their device
The elevators, the lighting, the HVAC, the timing all of that is will correspond to the meeting. Where the person goes will be watched and audited ..the meeting will be timed and video taped. all of this will happen with a single invitation being sent out
There may even come a time when your energy footprint is monitored by the access control devices and you may have it part of your performance plan.

Video

24

1. Crowd Sourced Camera's (google glass, contacts cell phones etc.)
2. Boston marathon bombing was one of the first to use crowdsourcing for forensic data. IAs you know…f something happens millennials and others are quick to whip out their phones and start shooting. A CCTV camera may be close…but not be getting the shot that is needed or wanted. But think of how many shots and angles people who are close to the incident could get.

- My prediction as to where this goes next. Inter-social Camera Utilization (ICU)…a person walks onto your campus, into your building, and immediately you can be grated access to a real time camera platforms (contacts/phones etc) and in an emergency your security group will be able to target an area and pull the feeds. Lot's of issues to consider here…but trust me it's coming (whether we are told about it or not)

Video

25

Finally Predictive emotional analytics (from angry emotions to happy, to sexual crimes) and others we are starting to see the emergence of technology that not only analysis behavior like we saw earlier but is analyzing emotion. Couple that with the huge amount of bio health devices that are about to flood the market and you have a recipe for pre-crime prevention ala minority report. Imagine a person coming into your building and their tagged as angry and watched more closely to be sure no issue arrises. the security staff then could react preemptively to mitigate a problem. We do this already innately as people, but as a security device it could be invaluable.

WRAPPING IT UP

26

The technology in physical security is starting to take tremendous strides. The conversation is moving from parts and pieces to networks and their infrastructure. As a wrap-up I want to talk about a small bump in the road that took place in 2010. a major manufacturer of security products was selling a network appliance that did not properly authenticate access to several directories, allowing an unauthenticated attacker to access network node logs, employee photographs, and backup archives. Access control (especially without your input) can put your companies data at risk. Though you might have different focuses…though you may have different personalities…we all need to make a spot for each other at the table so that we can effective protect our coworkers and our friend lives and data.