Impact of Technology on Today’s Security Guard Force

Mark Folmer, CPP, FSyI
VP, Security Industry
TrackTik
Impact of Technology On Frontline Security

Innovative Options to Drive Protection
Outline

- Why me?
- Security Planning
- Why the Frontline?
- Shift Thinking or Thought Shifting?
- Trends & Tech that Impact Service Delivery
- Tech for Tech Sake
- Digital Transformation
- Implementation and Change
- Wrap it all up
GOAL: Need to ensure this is the message

Modern security service providers can embrace various types of technology, service delivery methods and other business principles to deliver better service and to support the 5 Ds of physical security for practitioners.

The focus of this presentation is on sharing strategies, trends, and challenges addressing; speed/volume of data, budgets, business goals, exposure, and resource allocation.
Why Am I Here?

- Business
- Security Services
- Security Management Consulting
- Corporate Security
- Software guy
43% of security executives felt they didn’t receive enough funding “to administer a quality security process.”

When an incident happens – we need to know first:

- How severe it is?
- What is the impact across the organization?

Constantly challenged on:

- Are your resources the right ones?

Be able to roll them into corporate objectives – what is in it for me?

Managers “don’t know what they don’t know . . .”

Am I doing all I can do?
Security Expectations

- The lenses of the public
- Frictionless vs. convenience vs. Security
- Expectations
CEOs aim for growth, but eye tech for efficiency, cost management, productivity

Growth was cited as a top priority for 53% of CEOs, up 40 percent in 2018. Cost management also moved up the ranks in terms of priorities.

Source: Gartner (May 2019)
Back to Basics: Security Planning

**Deter**
Make the target so unattractive that the criminal goes elsewhere

**Detect**
If someone penetrates a secured area, ensure that they are spotted

**Deny**
Keep the bad folks out and allow the good people in!

**Delay**
If someone gets in, slow them down

**Defend**
Respond to a breach
Enterprise Security Risk Management (ESRM) is a strategic security program management approach that ties an organization’s security practice to its mission and goals using globally established and accepted risk management principles.
What is your Responsibility?

- **ESRM** recognizes that security responsibilities are shared by both security and business leadership, but that all final security decision making is the responsibility of the business leaders.

- The role of the security leader in **ESRM** is to manage security vulnerabilities to enterprise assets in a risk decision making partnership with the organization leaders in charge of those assets.
If you can only bring one thing to the party …
Data
Teams are a key component in the security arsenal as they help secure identified assets. On the flip side, security teams’ labour intensive composition also makes them expensive and in dire need of optimization.
Why the Frontline needs Change?

SECRET
Size
Spend
Pains
Security Magazine:

The “new security company” must adapt to changing customer requirements, demographic developments and technological advances if it wants to remain successful ... ”
Setting Expectations Higher?

- Security guard forces, and the methods used to manage them, have seen transformational change in recent decades. Twenty years ago, the tools of the trade were a notepad and a pen, and the required technical skills peaked with the ability to use a handheld two-way radio…

- Guard force security was not viewed in a professional manner; guard jobs were often considered “no specific skills needed” entry-level positions. Recruiters frequently told applicants, “if you can stay awake, you can do this job”.


The competition: Cyber is Sexy

Does it need to be one vs. the other?
It Ain’t about the Tech!

- **82%** of CEOs has a digital business or transformation effort underway.
- **27%** of CEOs were looking toward technology as a way to manage and control costs.
- **47%** saw technology as a way to boost productivity.
- **18%** of CEOs saw talent management as a skill to improve with 17% citing digitization and technology enablement and 15% noting data management.
Understand Tech Impact
People, Process, Technology
Define Innovation

Electricity is much more than the evolution of the candle, consider how that applies to: guns, gates, guards?
Industry 4.0

“Accelerating technological advancement is transforming our world and our core business of physical security is just one dimension of our increasingly expansive sector. We need a diverse range of perspective, skills and experience within our field to equip us for the challenges and opportunities to come.”

Dr. Alison Wakefield
Chairman, Security Institute
Shift thinking
Digital Transformation Tips

- “Digital transformation marks a radical rethinking of how an organization uses technology, people and processes to fundamentally change business performance” says George Westerman, MIT principal research scientist and author of *Leading Digital: Turning Technology Into Business Transformation*

- 89% of security leaders in the Microsoft Accenture report consider the digital transformation to be “important”; 30% of these “urgent”

- ROI and non-financial benefits to be expected
Connect the dots

- How do these impact frontline services?
- Ask yourselves the question: what can I do better?
- Harken back to the comment re: innovation – what is it really in my case?
Tech as Guard Force Multipliers

- License Plate Recognition
- Facial Recognition
- Access Control Readers
- Workforce Management
- Artificial Intelligence
UAV or UxV
Remote Video Monitoring
Data Collection
Artificial Intelligence / Machine Learning
Facial Recognition

- $9 Billion mkt by 2025
Impact Guard Retention!
Delivery of services
Measuring ROD

- Security economics suggests: one is better off with real numbers to measure the likelihood and the magnitude of risk.
- The top security investment in the next 3-5 years, according to 83% of security leaders, will be big data and analytics (Microsoft Accenture)
Change:

Tech for tech sake vs. tech with a plan

- Analyze your requirements
- Executive buy-in
- Plan & budget for tech
- A-level team
- Best software & technology fit
- Test the solution
- Thoroughly search for vendors
Consider

- Compliance
- Crossover of Infosec and Physec
- Need for greater internal controls
- Convergence between Physec, Infosec & Cybersec
Reflections from a CSO Summit

- Engage other departments
- Opportunity to Impact
- Add value
- Be agile
- Execute through others
- Connect in every direction
- The multi dimensions of risk
- Bring numbers to the party
- Social Media growth by 320 million UPY
- Lenses
- Create Value where it does not exist today
- Finding intersections
- Risk is a board level issue
Takeaways

Efficiency

Insight

Deliver value
Benefits of getting it right!

- **Thinking long-term:** in a perfect world, security solutions shouldn’t be driven by media pressure, isolated events or budget constraints; in line with best practice, decisions should be with a long term strategic viewpoint, utilising the knowledge and experience of specialist experts, industry bodies and comprehensive risk analysis.

- In order to effect change, **security** will need to be considered on equal standing with other factors such as sustainability. Without embedding security at the earliest stages of the design process, projects risk poorly implemented security measures, inappropriate budget, corner cutting and increased costs in the future.
Thank You!

Mark Folmer, CPP, MSyI
Vice President, Security Industry
mark@tracktik.com
linkedin.com/in/markfolmer | twitter.com/markfolmer