Secure Digital Transformation

Turning the dream into a reality

David Millar-LaRocque
Canadian Solutions Leader
Digital transformation is the complete reorganization of your business processes and even business model to positively affect your specific organization and society in general.
It isn’t just moving stuff to the cloud, agility is table stakes.
The change will improve the collection and use of data to create a competitive advantage or barriers to entry.
The collection, use, governance and disposal of this data must be done securely.
There are a number of barriers to achieving a successful secure digital transformation.

- 56% Complexity of the business processes
- 50% Insufficient visibility of people and business processes
- 47% Lack of skilled or expert personnel
- 44% Lack of effective security technology solutions

Bridging the Digital Transformation Divide: Leaders must balance security & growth, Ponemon Institute, Mar 2018
There were a number of challenges identified also...

61% Continuous availability of IT infrastructure

57% Limiting unauthorized access to data and applications

47% The ability to use sensitive or confidential information to improve the customer experience

46% The ability to overcome turf and silo issues

43% The ability to avoid security exploits and data breaches

Bridging the Digital Transformation Divide: Leaders must balance security & growth, Ponemon Institute, Mar 2018
Security teams are already firefighting and face an onslaught of challenges

Large skills gap in security expertise worldwide

Too many tools to manage effectively

Increased volume and attack sophistication
At current course and speed, your security organization will **not** be able to keep up with the demands of your business.
You will need AI² to transform with your organization’s digital transformation.
Artificial Intelligence is "the capability of a machine to imitate intelligent human behaviour."
79% Technologies that utilize machine learning/artificial intelligence for cybersecurity will help secure the transformation
Adding Artificial Intelligence to your security organization will improve its *effectiveness*.

- **69%** Increases speed of analysing threats
- **60%** Increases productivity of your personnel
- **63%** AI users are able to detect more ‘un-detectable’ threats

*Foresight Institute Study: “The Value of AI in Cybersecurity”, 2018*
Purchase solutions from vendors that embed AI to address specific use cases that align with your threat/risk goals and demonstrates improved productivity and/or improved threat detection.
Aggregate the output of those AI solutions – along with your enterprise system logs and security event data – into a Security Intelligence platform that also leverages AI to improve threat response.
Purchase MSS services from a vendor who uses Artificial Intelligence to improve your service.
You will need to start looking for ways to build *custom AI* solutions leveraging the new data from across the organization to detect security threats, fraud, and other costly behaviour.
52% of respondents in the Ponemon study say that AI will drive a greater demand for full time, dedicated headcount.

This new AI enabled organization will need Data scientists, Business Analysts, Risk analysts, Compliance specialists, SME’s, programmers, app developers, and many more!

Ponemon Institute Study, “The Value of AI in Cybersecurity”, 2018
Where are we going to find all of these people?
You need to look for **AI** to *staff* your program.
Alternative Intelligence is “relating to the ability to acquire and apply knowledge or skills that is considered unconventional and as a challenge to traditional norms.”
Here are some examples of people who thought differently...who possessed ‘alternative intelligence.’
“Asperger syndrome (AS), also known as Asperger's, is a developmental disorder characterized by significant difficulties in social interaction and nonverbal communication, along with restricted and repetitive patterns of behavior and interests.”
Focus on the details

Original way of thinking

Independent

Intensity

Honest

Not swayed by Social convention

Pattern Recognition
There are 350,000 autistic adults in Canada.

85% of them are unemployed or underemployed.

Data from Specialisterne Canada
Our recruitment processes are broken.
• How you look
• Eye Contact
• Body position
• ‘in synch’
• Are your answers socially acceptable
• Comparing to previous interviews
• Higher weighting on negatives
• Are they ‘like me’

Interviews are biased and are a terrible predictor of job success.
And these interview bias, stop people on the spectrum in their tracks.
“Shawn’s talent and unique eye for problem solving and detail, has helped propel our program further than we could have imagined. Today, I find that the team works better together, forming a cohesive and diverse unit that is much more adept at tackling dynamic information security issues.”

Mihai Saveschi, Director of Information Security
Your recruitment process
your heart and
finally on
first in your mind, then in
You must open the aperture
To achieve SECURE digital transformation, you need AI\(^2\) to evolve your cybersecurity program.

**Alternative Intelligence**
- Autistic adults
- Cyber Security
- Data Scientists
- Process specialists
- Business Analysts
- Risk Analysts
- Audit & Compliance

**Artificial Intelligence**
- Black box AI for specific Use cases
- AI at the Enterprise SIEM layer
- MSS Provider to focus efforts on real threats
- Custom AI
Link to the Ponemon Digital Transformation Report here.

Link to Ponemon AI report Here.

Connect with me on LinkedIn or Email

Reach Specialisterne here or connect with Alan Kris, CEO on LinkedIn here
THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions