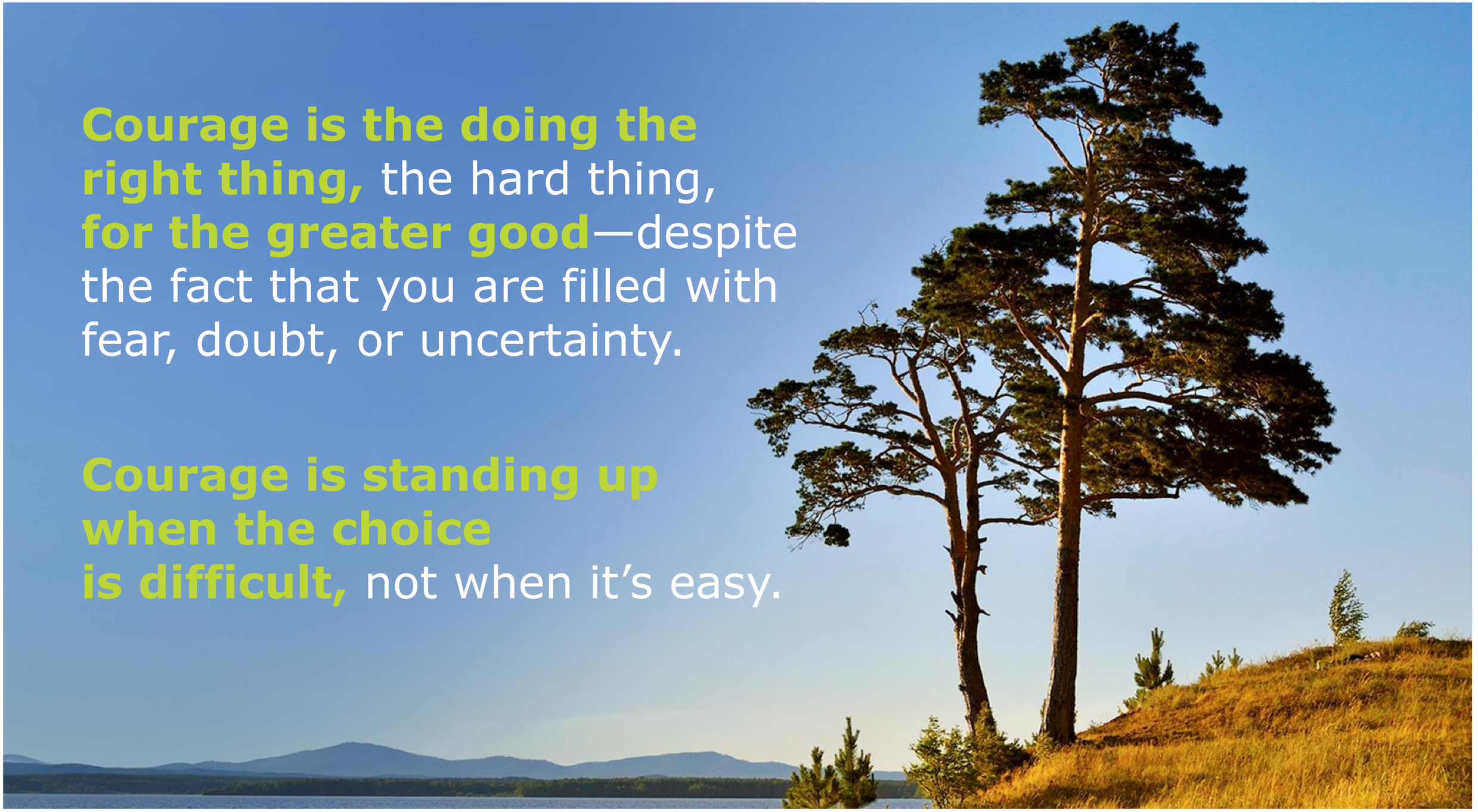
1:00 – 1:40

Deloitte.

Cyber Security in a world of AI & Automation and the courage to go forward

OCIO Security Day – November 2018

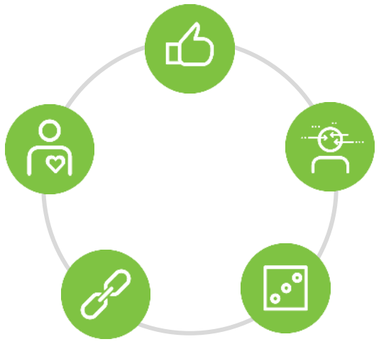
CANADA AT 175


Courage is the doing the right thing, the hard thing, **for the greater good**—despite the fact that you are filled with fear, doubt, or uncertainty.
Courage is standing up when the choice is difficult, not when it’s easy.

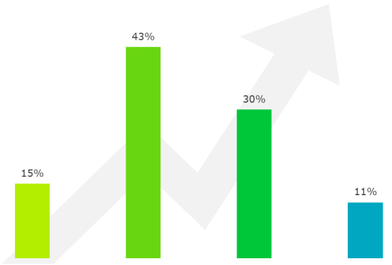
Assessing courage and its impact

We surveyed 1,200 Canadian leaders and evaluated the level of courage in their organizations.

We designed and deployed a survey that evaluated 1,200 Canadian businesses on the five elements of courage.



A framework was developed to segment the survey respondents by courageousness.

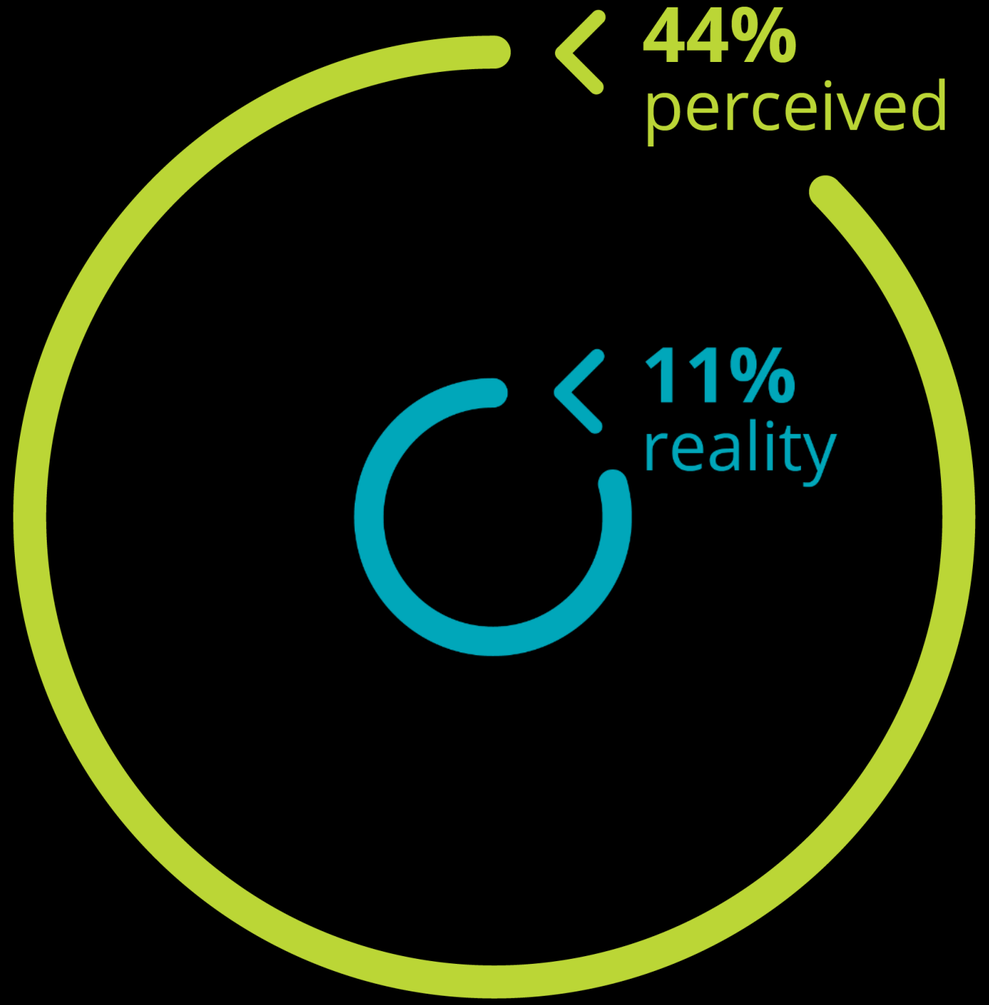


The impact of courage on business outcomes was evaluated using survey questions aimed at measuring respondents' businesses performance.

Today, only Canadian businesses can be considered **one in ten truly courageous.**

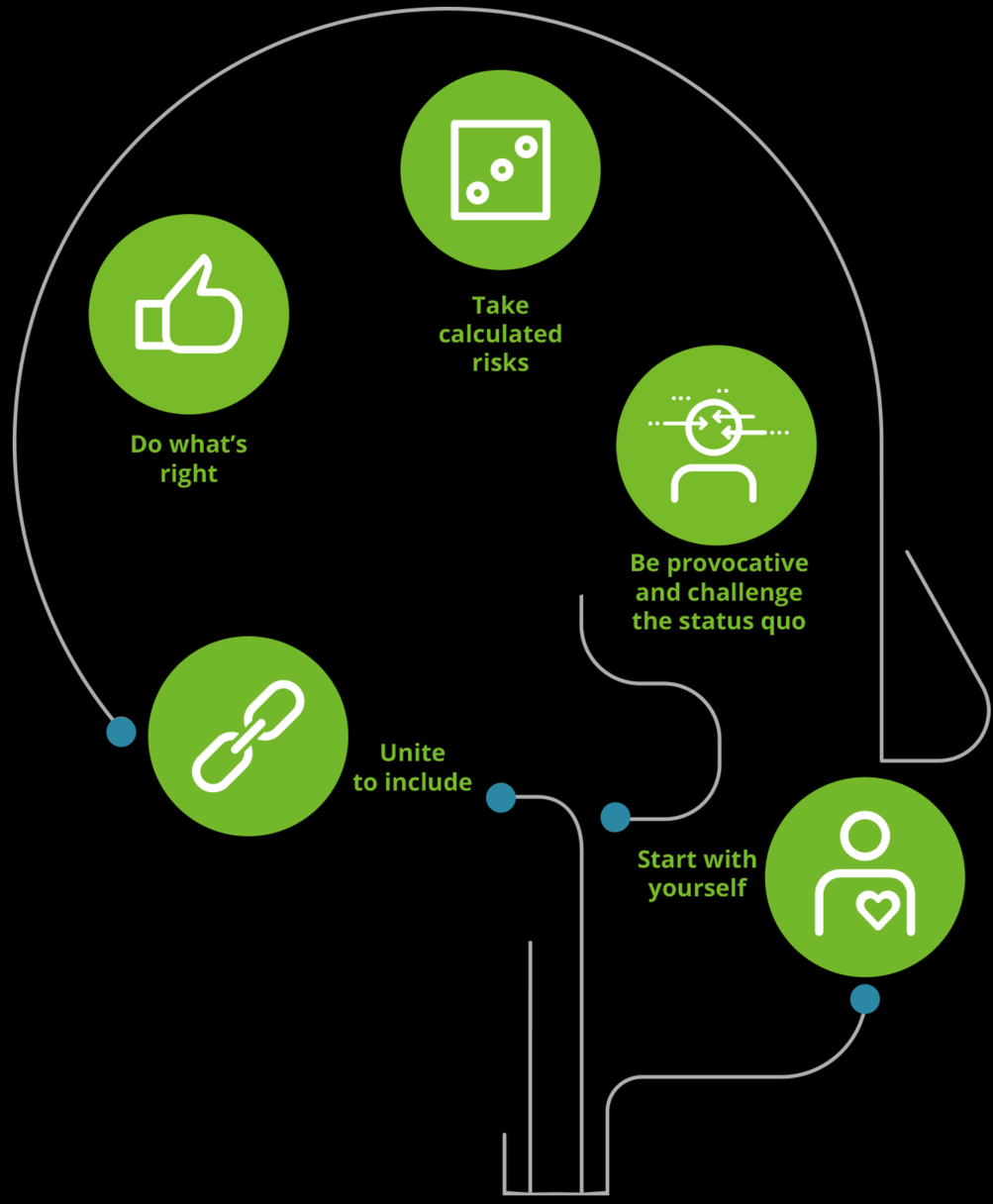
Even more interesting is our lack of awareness.

Canadian businesses believe they are four times more courageous than they actually are.



Courage makes a difference—courageous organizations **grow faster**, and **pursue growth more aggressively.**

Through our research, we have come to understand that courage is comprised of **five elements.**



Be provocative and challenge the status quo

1 Understand your organization’s value proposition in its simplest form.

2 Change your customers’ understanding of what they need.

3 Seek out opposing views.

Take calculated risks

1. Reframe risk as a positive indicator of courageous decision-making.
2. Incentivize courageous risk-taking.
3. Let business imperatives—not fear—dictate your risk threshold.

Do what’s right

1 Share your strengths.

2 Become a partner in building the kind of economy Canada needs.

3 Focus on long-term growth and market leadership.

Start with yourself

1 Let your vision and mission guide you.

2 Take responsibility for the actions you care about.

3 Hold yourself accountable.

Unite to include

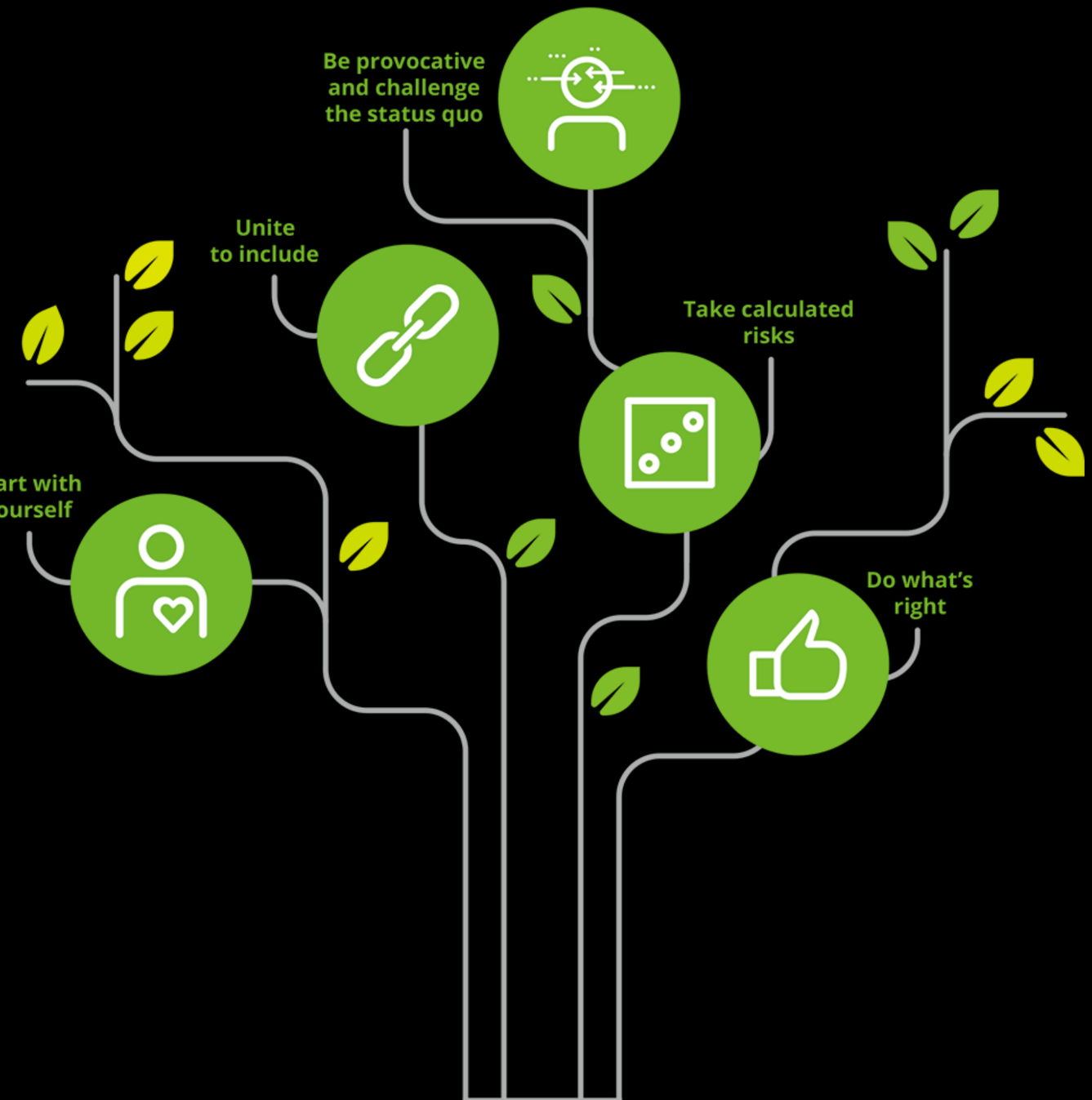
1 Start a dialogue with employees at all levels of the organization.

2 Make inclusion a priority.

3 Recognize the ripple effect of your network.

Organizations should start by **understanding** their current position.

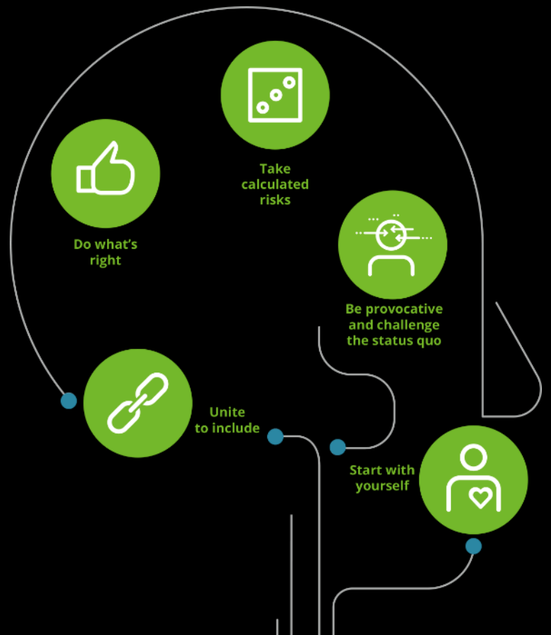
Then, leaders must **prioritize** the elements with which they struggle.



Courage self-assessment:

How does your organization stack up?

www.canada175.ca/en/courage-self-assessment

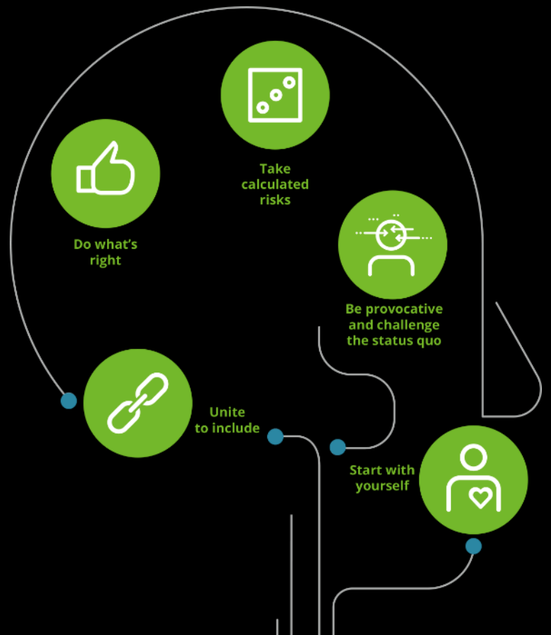


1. What is your organization’s risk tolerance?
2. How much flexibility do your employees have to undertake initiatives not directly related to their work mandate?
3. How accurately does *“brings diverse perspectives to decision-making”* describe your organization?
4. How accurately does *“has a vision and purpose”* describe your organization?
5. How accurately does *“leverages individuals unique strengths and qualifications when forming teams”* describe your organization?

Courage self-assessment:

How does your organization stack up?

www.canada175.ca/en/courage-self-assessment



6 How accurately does *"Challenges convention"* describe your organization?

7 To what extent do your personal and moral beliefs influence your decision making?

8 To what extent do long term returns influence your decision making?

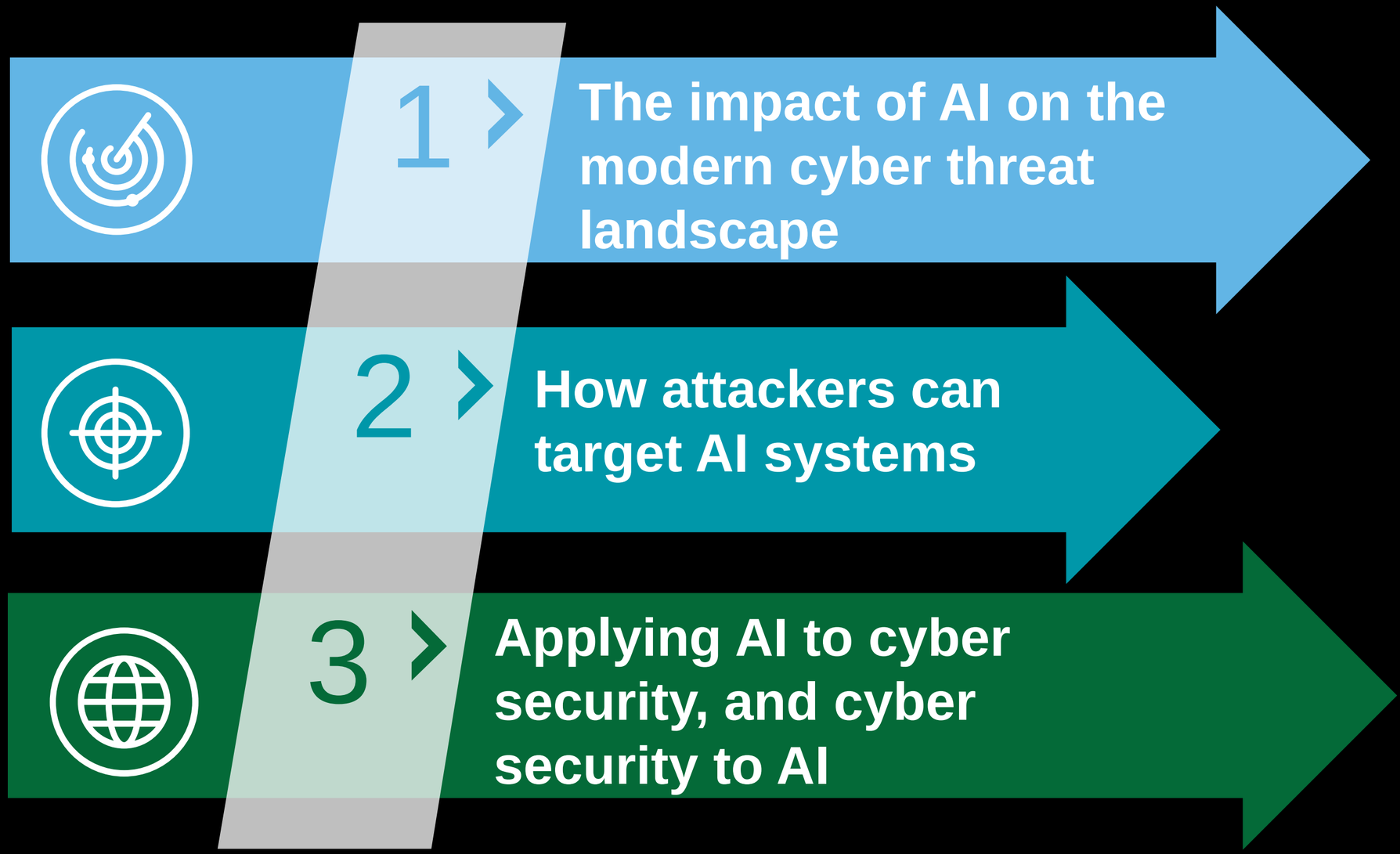
9 To what extent does societal good factor into the vision and strategy of your organization?

10 To what extent does input from junior level employees influence your decision making?

Deloitte.

Cyber Security
in a world of AI & Automation

Agenda



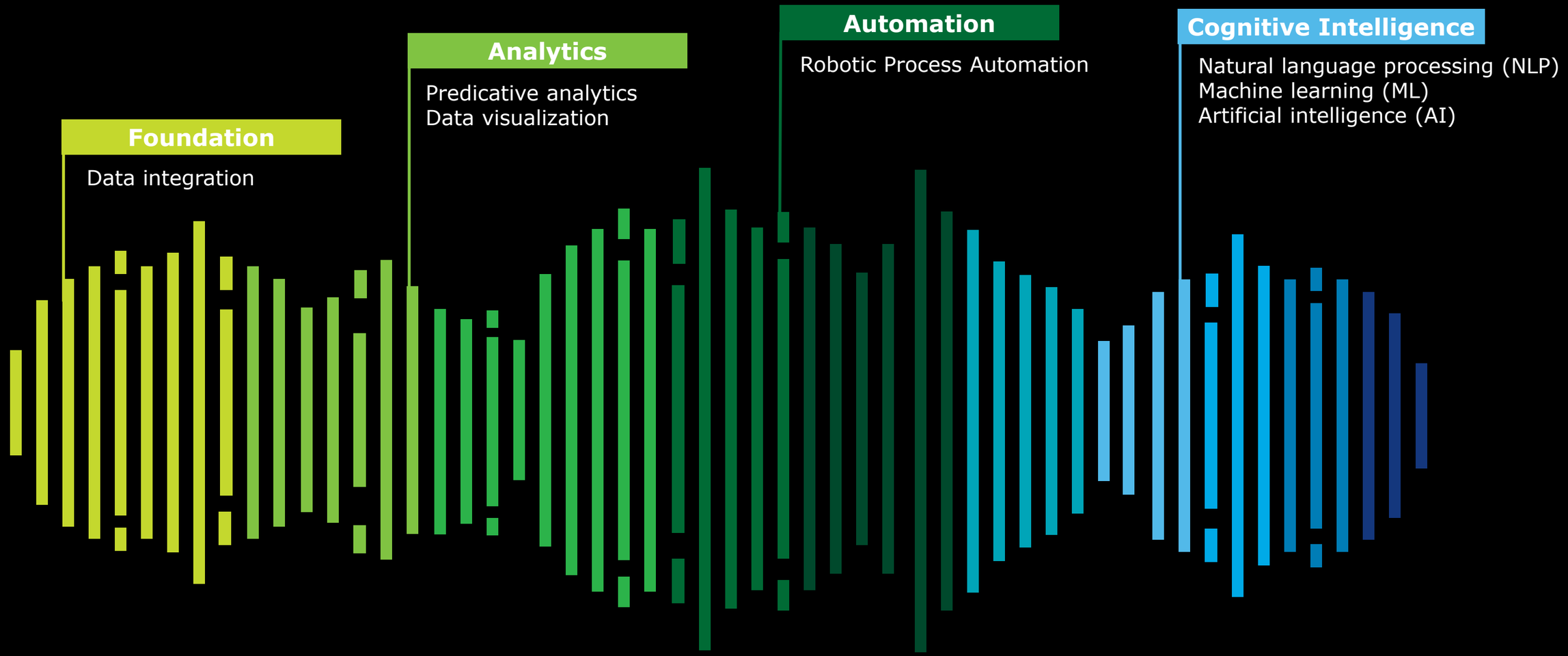
+ AI’s DANCE CARD

AI is likely to be either the best or worst thing to happen to humanity

Stephen Hawking

Deloitte.

The digitization spectrum



+ THE CYBER LANDSCAPE

For the newly emerging digital world, cybersecurity needs to be reimagined.

Forbes

Major cyber threat trends

Global Cyber Insight 3 – Heightened Caution on use of Identities

Due to the recent disclosure of data breaches, enterprises are advised to employ heightened situational awareness on user account takeover and mis-use.

Global Cyber Insight 2 – Cloud Exploitation

With the increasing adoption and use of extended enterprise (SaaS, etc), Deloitte's Cyber Threat Intelligence team is intercepting increasing activity and methods targeting cloud based applications and security measures.

Global Cyber Insight 4 – Next Generation Ransomware

Anticipated threats against organizations utilizing Next Generation Ransomware.

Global Cyber Insight 1 – Financial Sector Targeted

Actors continue to steal considerable amounts of funds from international banks and other associate FSI organizations. Abuse of SWIFT protocol, use of leaked exploits, and phishing campaigns remain as preferred compromise vectors.

Global Cyber Insight 5 – Increasing Web Application Exploits

Heightened use of exploit techniques against Apache and other Web Based Application servers.

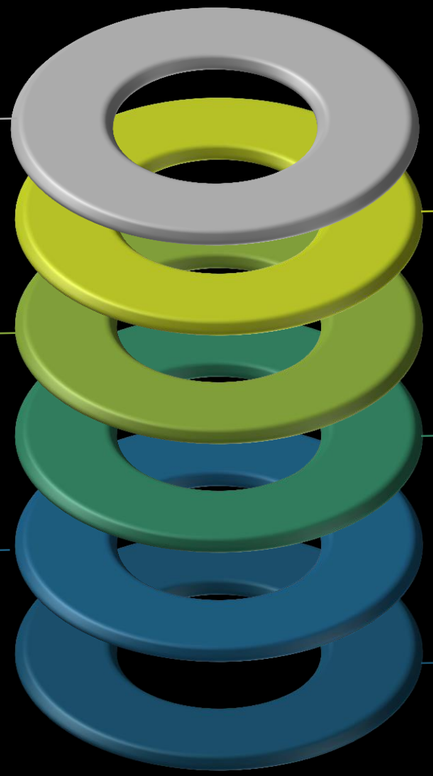
+ A DOUBLE-EDGED SWORD

AI as a “dual use technology” with potential military and civilian uses, akin to nuclear power, explosives

The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation

Deloitte.

The double-edged properties of AI



AI is dual-use

AI is efficient and scalable

AI can exceed human capabilities

AI increases anonymity and distance

AI software and research is easy to access

AI systems suffer from unsolved vulnerabilities

AI growth and spread will introduce shifts in the threat landscape:

- Existing threats will grow:
  as the cost to execute increases, the actors, rate of attack and range of targets will rise.
- New threats will arise:
  the use of AI will provide attackers with access to tools and methods that would have otherwise been impractical. In addition, AI systems themselves open new avenues for attack.
- Threats become more effective
  the growing use of AI will increase efficacy of both the attack and target identification.

+ ATTACKING AI

Artificial Intelligence has the same relation to intelligence as artificial flowers have to flowers

David Parnas

AI is not mathematics – it is trained decision making

Deep learning is powered by the ever-growing set of data and the increase in computational power, but whereas a cat is a cat, attacks are always evolving.

Hackers can foil AI algorithms

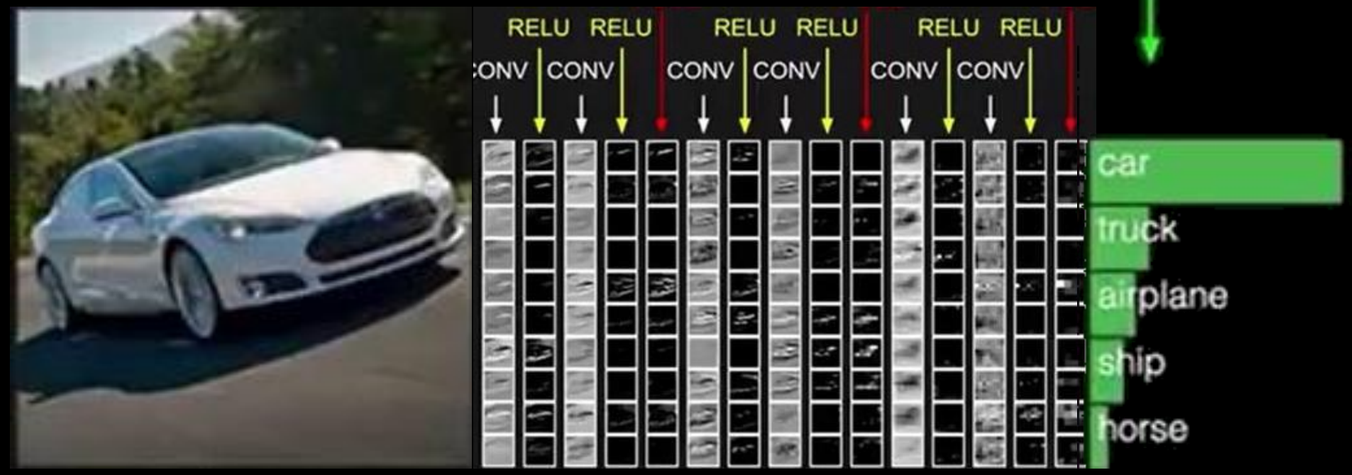
By targeting the data they train on and the warning flags they look for, attackers don’t even need to tamper with the data; instead, they could work out the features that a model is using and then remove these from their behavior.

Banana

Toaster

AI decisions also lack context

Over the years, image classification has become super-efficient and outperforms humans in many settings. This doesn't mean the algorithms understand the context of images the same way that humans do, though



+ EXAMPLES IN THE WILD

Within three years enterprise intelligent assistants will be the primary point of contact to support real world commerce.

Dan Miller, Founder, Opus Research

‘Tay Bot’—a case for cautious machine learning

An AI chatbot created by Microsoft’s AI research team was the victim of coordinated attacks to ‘mis-train’ it.

Common AI attack techniques include:

- Adversarial inputs
- Data poisoning attacks
- Model stealing techniques

+ AI RELIES ON BIG DATA

Information is the oil of the 21st century, and analytics is the combustion engine.

Peter Sondergaard

Deloitte.

AI and ML challenge the rules of data security

Machine learning tends to require a lot of data. Training a machine learning model might require millions of data elements. While machine learning requirements vary based on the use case, "acquiring and labeling data can be time-consuming and costly."

Large amounts of business data is involved, which can hold significant value (e.g., past transactions at a brokerage) or sensitivity (e.g., medical records from a chain of hospitals).

Learning datasets often include all attributes/aspects (dimensions) of data, which conflicts with the ‘data minimization’ principles of privacy.

Unlike traditional software engineering, machine learning cannot always use ‘dummy data’. Deloitte has found that while it is possible to use limited real data, a large portion must remain real.

Deloitte.

+ CYBER ANALYTICS

Speed, the tempo of decision and information is the problem, because our adversaries have figured out how to move inside our decision loop.

Pamela Melroy, former space shuttle commander and deputy director of DARPA's Tactical Technology Office

AI applied in the kill chain

AI exploits are not only able to find new ways to discover vulnerabilities, but they can also identify which data is more important to a breach.

Discovery
Checking for vulnerabilities, fuzzing, morphing and limit testing

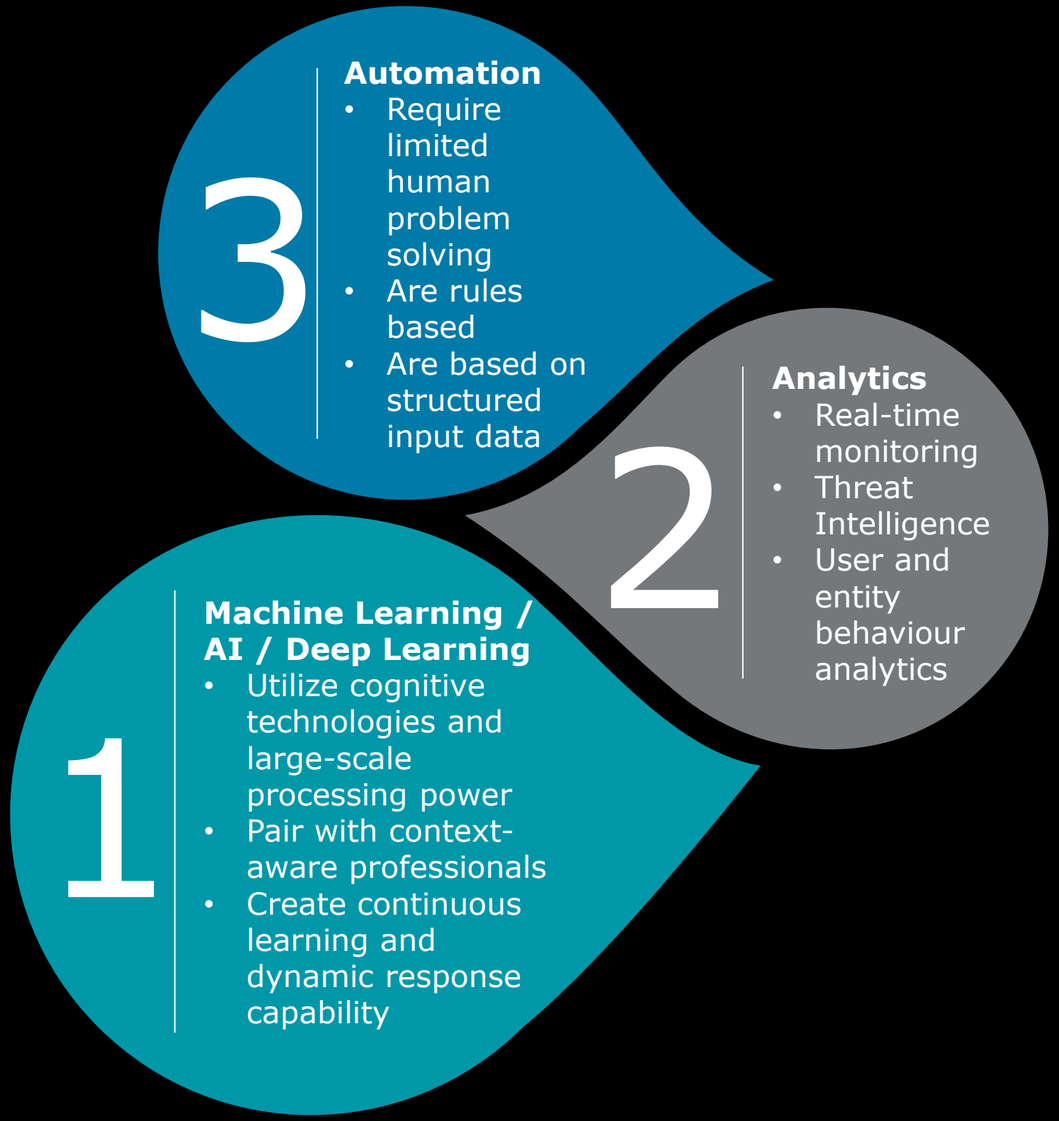
Weaponize
Generating payloads that evade common detection measures through testing

Exploitation
Automation and near-real-time adapting of attacks, as well as recursive exploitation

Actions and Objectives
Hunting for the most critical assets through intelligent and automated searching

Analytics & machine learning for effective cybersecurity

Separating the signal from the noise, drawing meaningful insights from large volumes of technical and risk data, identifying deviations from the norm.



Key considerations

- Analytics is a foundation for effective security, but continued focus on the fundamentals is important
- Automation, analytics and AI are key cybersecurity enablers but people remain a critical element
- Context is key - target analytics efforts based on risk, industry and organizational context to ensure insights are relevant and actionable
- When deploying analytics monitor and “tune” your approach over time to ensure relevance and business value

+ SECURING AI

There is no free will in what we create with AI. Everything functions within rules and parameters

Clyde DeSouza

Some guiding principles apply to AI implementation security

Have a good data governance structure is in place. AI, ML and DLN leverage large and valuable sets of data.

Perform diligent threat modeling of solutions—both at component level and from an end to end perspective.

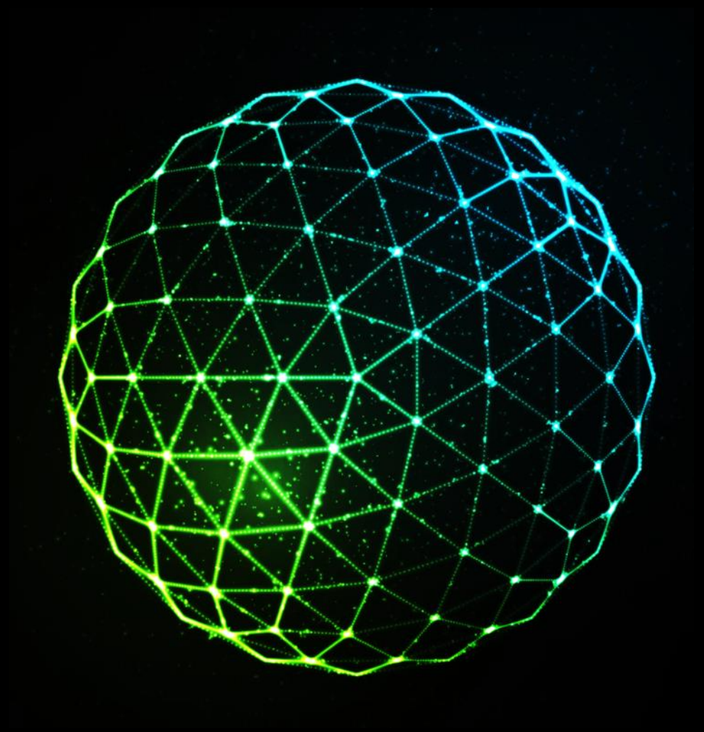
Ensure that good programming practices are followed during implementation, using verified components and reputable developers.

Machine learning algorithm “hyper-parameters” should be protected from tampering, exposure or manipulation, wherever they may reside.

AI requires significant compute power, and this offers significant value to attackers. Securing this infrastructure is a top priority.

Joyce Drohan
Partner | Deloitte
BC Practice Leader for Omia AI

Robb Anderson
Senior Manager | Deloitte
Risk Advisory - Cyber Risk



Headline Verdana Bold

Questions and Answers

Deloitte.

CANADA AT 175

OCIO Security Day – November 2018