BEAUCERON

Patching Your People:
Building the Sheepdog Effect

About David

- Bachelor of Arts, Information and Communications Studies
- Master of Business Administration
- Certified Information Security Manager
- Former journalist, soldier
- Lifelong nerd

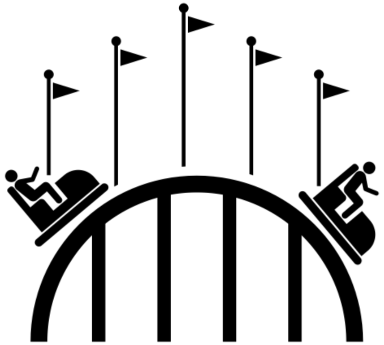
BEAUCERON

Work @UNB

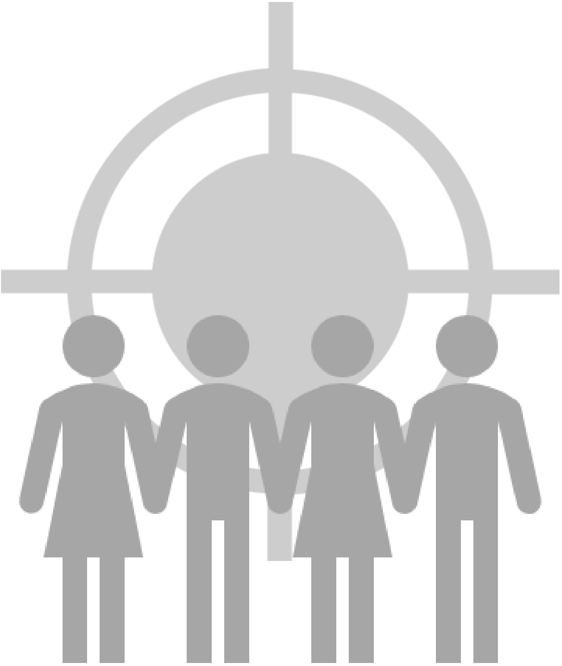
- Had an LMS-based awareness campaign (voluntary, low uptake)
- Used SaaS phishing tool that required manual effort
- Responded to dozens of incidents per week
- Responsible for reviewing SIEM data, threat intel
- Part of long-term strategic risk reduction project

BEAUCERON

Organized Crime



Thrill seekers



95%

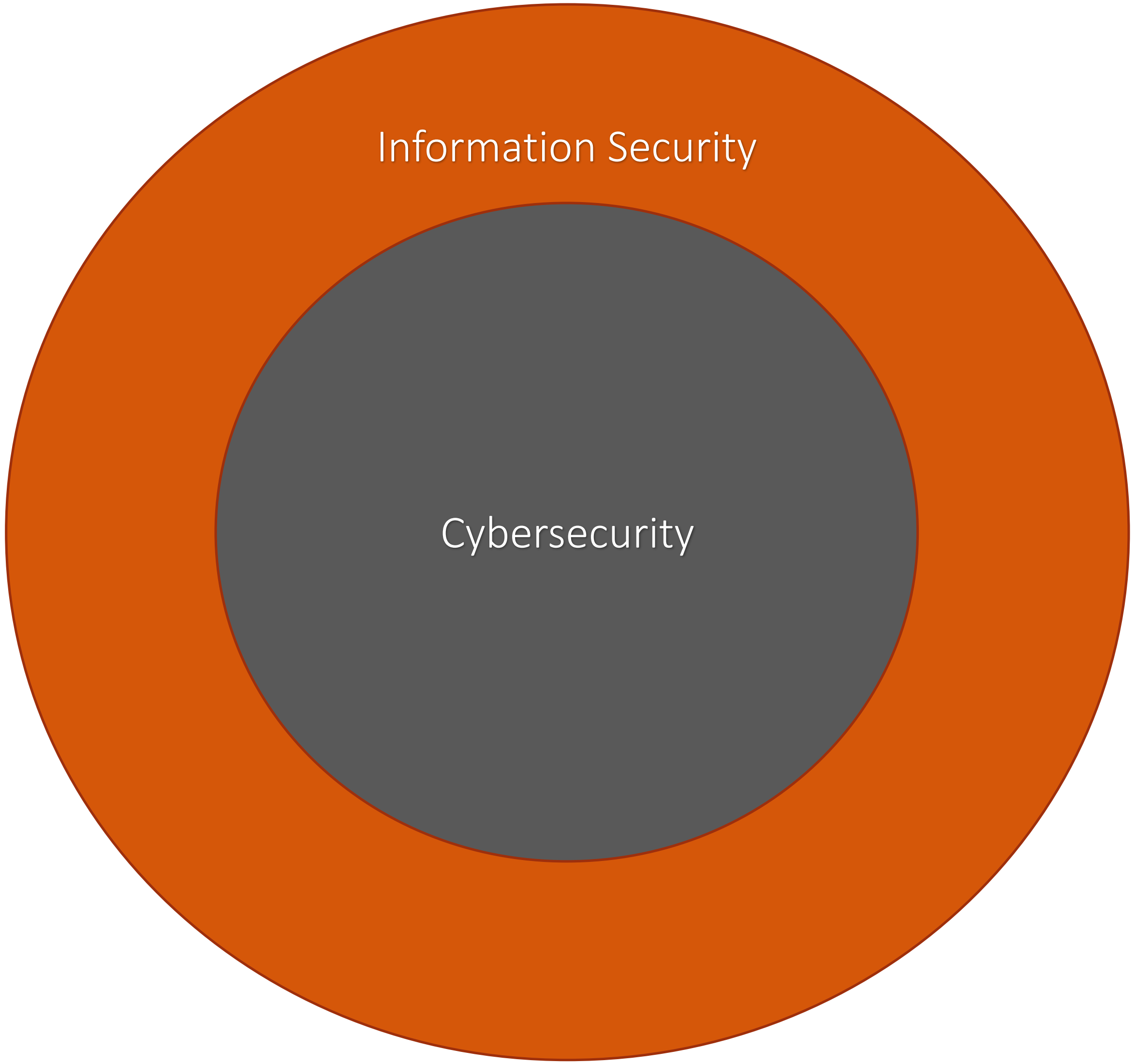
Hacktivists

Nation-states

Core problem: Time

- Did not have enough hours in the day to run an effective behaviour change program and perform other duties
- At the same time, attacks against UNB were surging with people, process and culture as common elements in nearly all incidents
- Needed a way to automate and scale

BEAUCERON



Information Security vs Cybersecurity

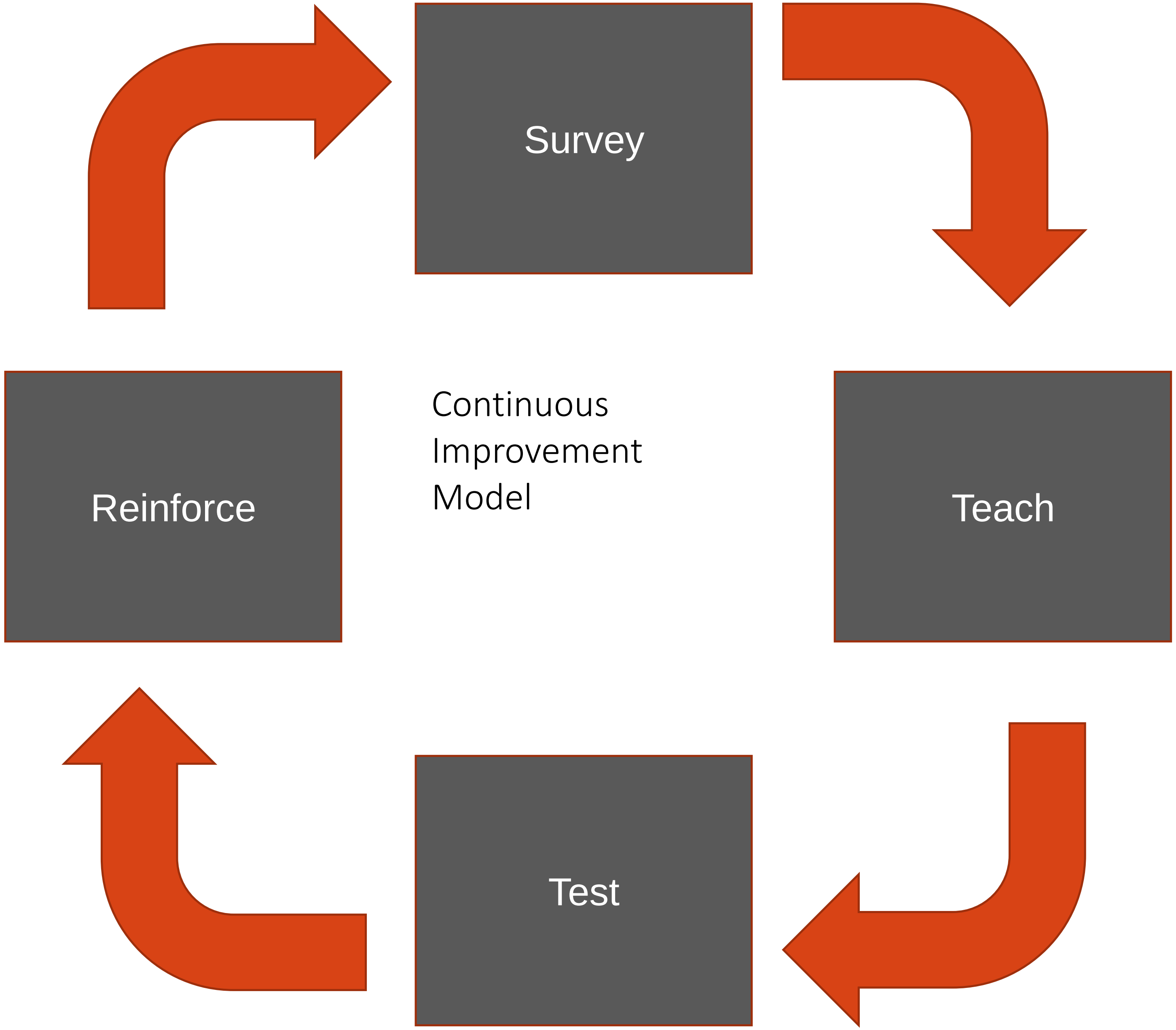
Cyber

BEAUCERON

Cyber history

- “Cyberspace” - William Gibson, ‘82 – Burning Chrome
- Cybernetics – Norbert Weiner, 1948
- Kybernḗtēs – Greek for steersman or helmsman

Model behaviour



Survey

Teach

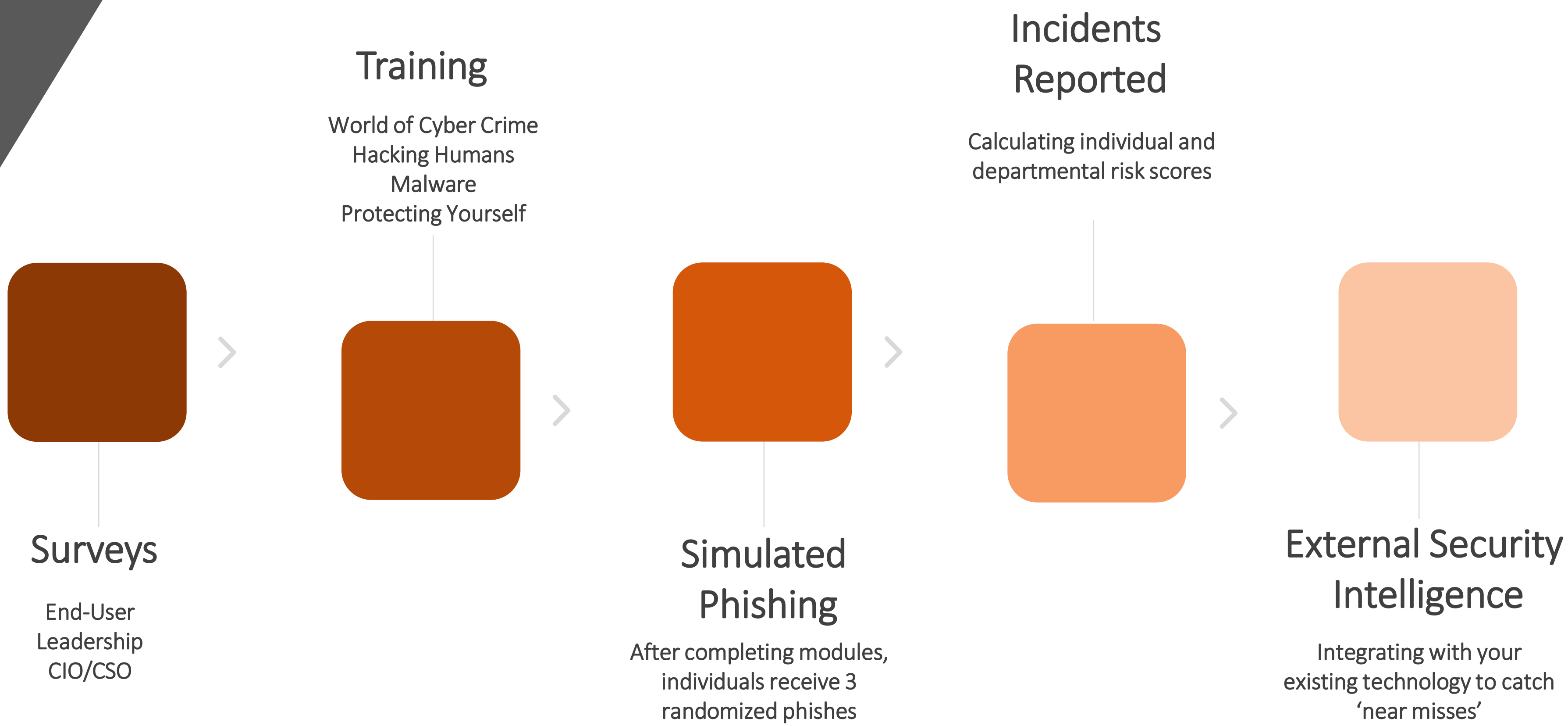
Test

Reinforce

Continuous
Improvement
Model

BEAUCERON

Human-Centric Approach



Surveys

End-User
Leadership
CIO/CSO

Training

World of Cyber Crime
Hacking Humans
Malware
Protecting Yourself

Simulated Phishing

After completing modules, individuals receive 3 randomized phishes

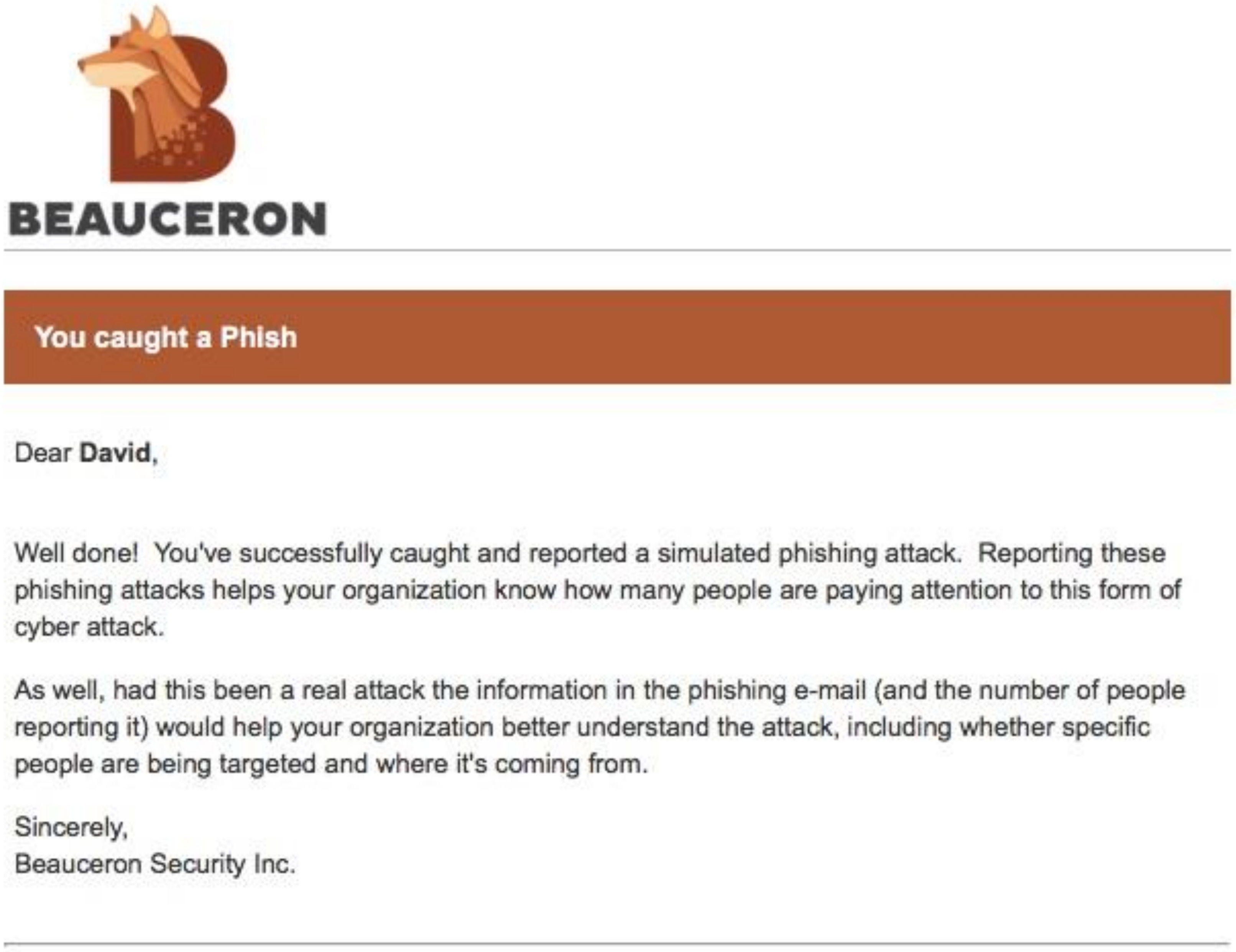
Incidents Reported

Calculating individual and departmental risk scores

External Security Intelligence

Integrating with your existing technology to catch ‘near misses’

Rewards



BEAUCERON

You caught a Phish

Dear **David**,

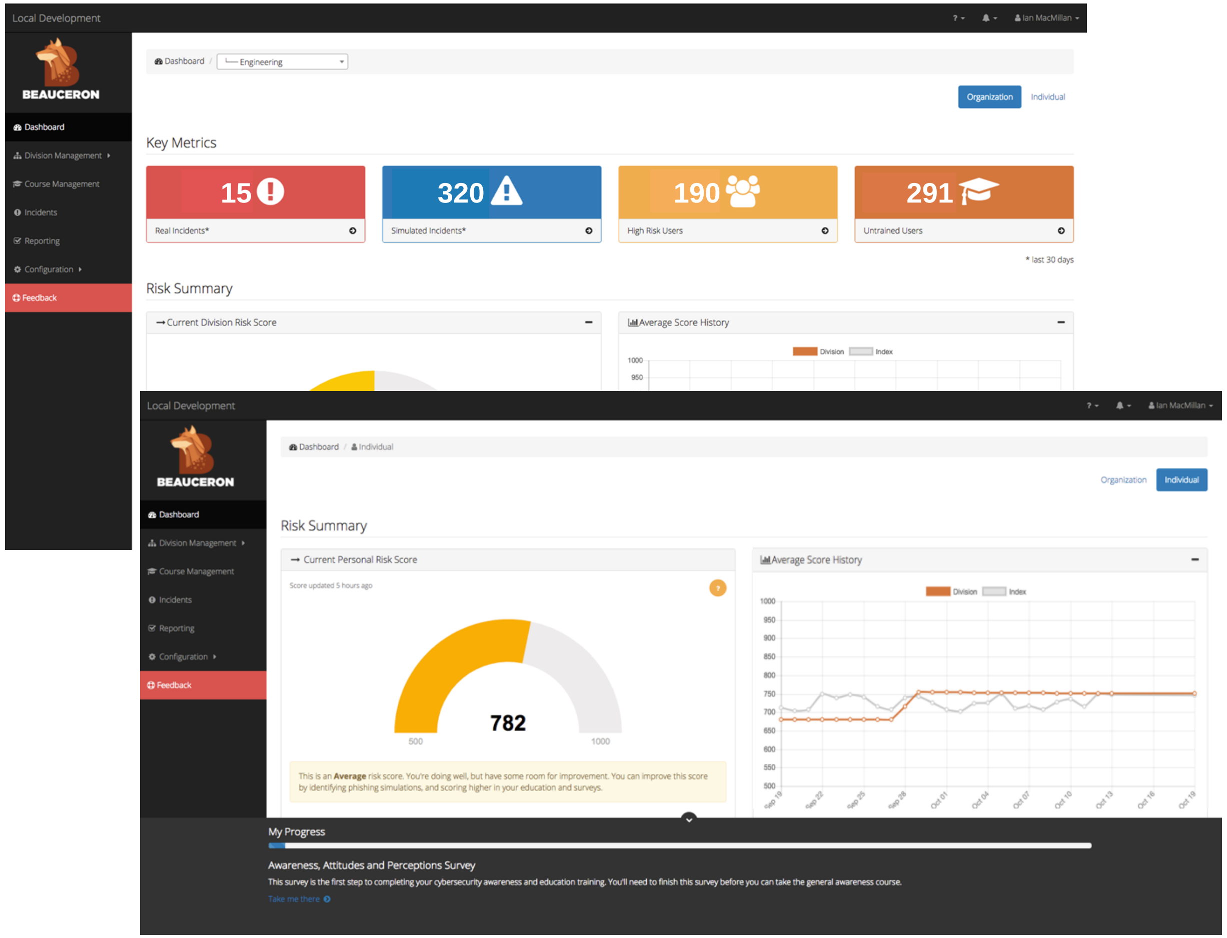
Well done! You've successfully caught and reported a simulated phishing attack. Reporting these phishing attacks helps your organization know how many people are paying attention to this form of cyber attack.

As well, had this been a real attack the information in the phishing e-mail (and the number of people reporting it) would help your organization better understand the attack, including whether specific people are being targeted and where it's coming from.

Sincerely,
Beauceron Security Inc.

Technology

- Software-as-a-Service
- Cost-effective
- Easily scalable and sustainable
- Safe and Secure



This is an **Average** risk score. You're doing well, but have some room for improvement. You can improve this score by identifying phishing simulations, and scoring higher in your education and surveys.

Awareness, Attitudes and Perceptions Survey

This survey is the first step to completing your cybersecurity awareness and education training. You'll need to finish this survey before you can take the general awareness course.

BEAUCERON

Office 365

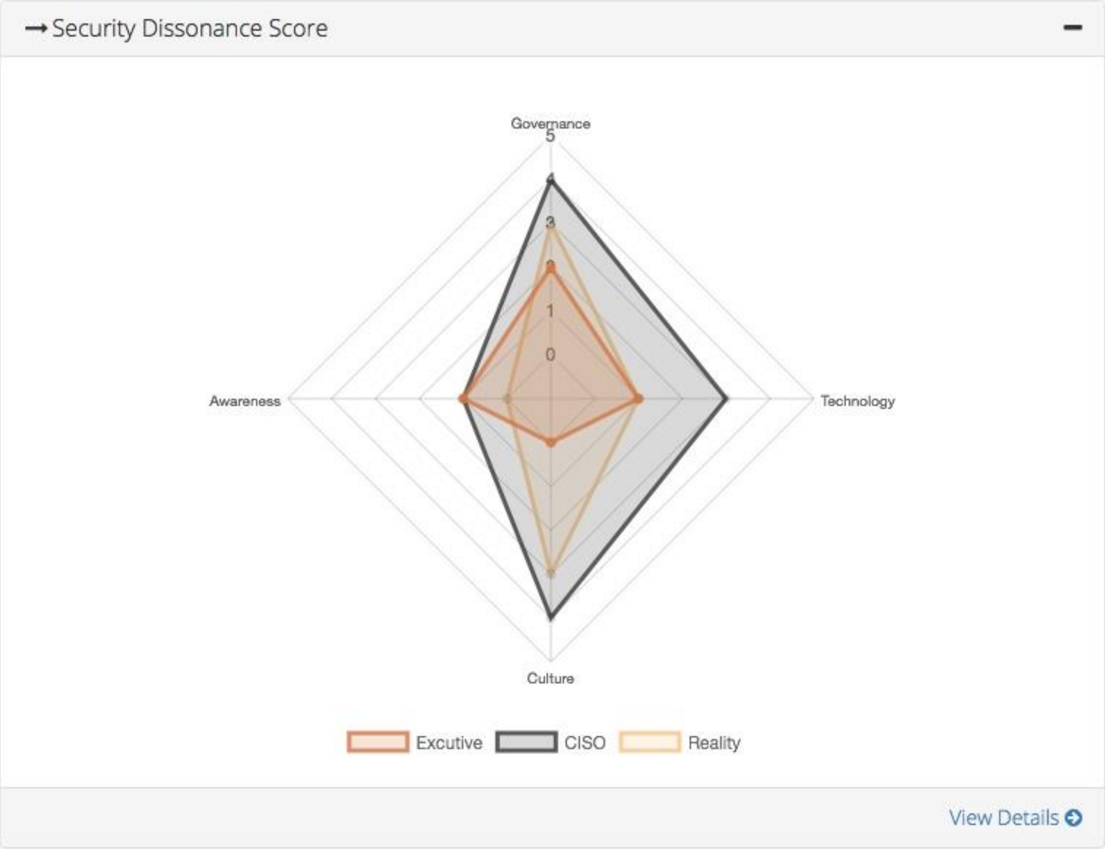
Microsoft Azure

Changing Culture

BEAUCERON

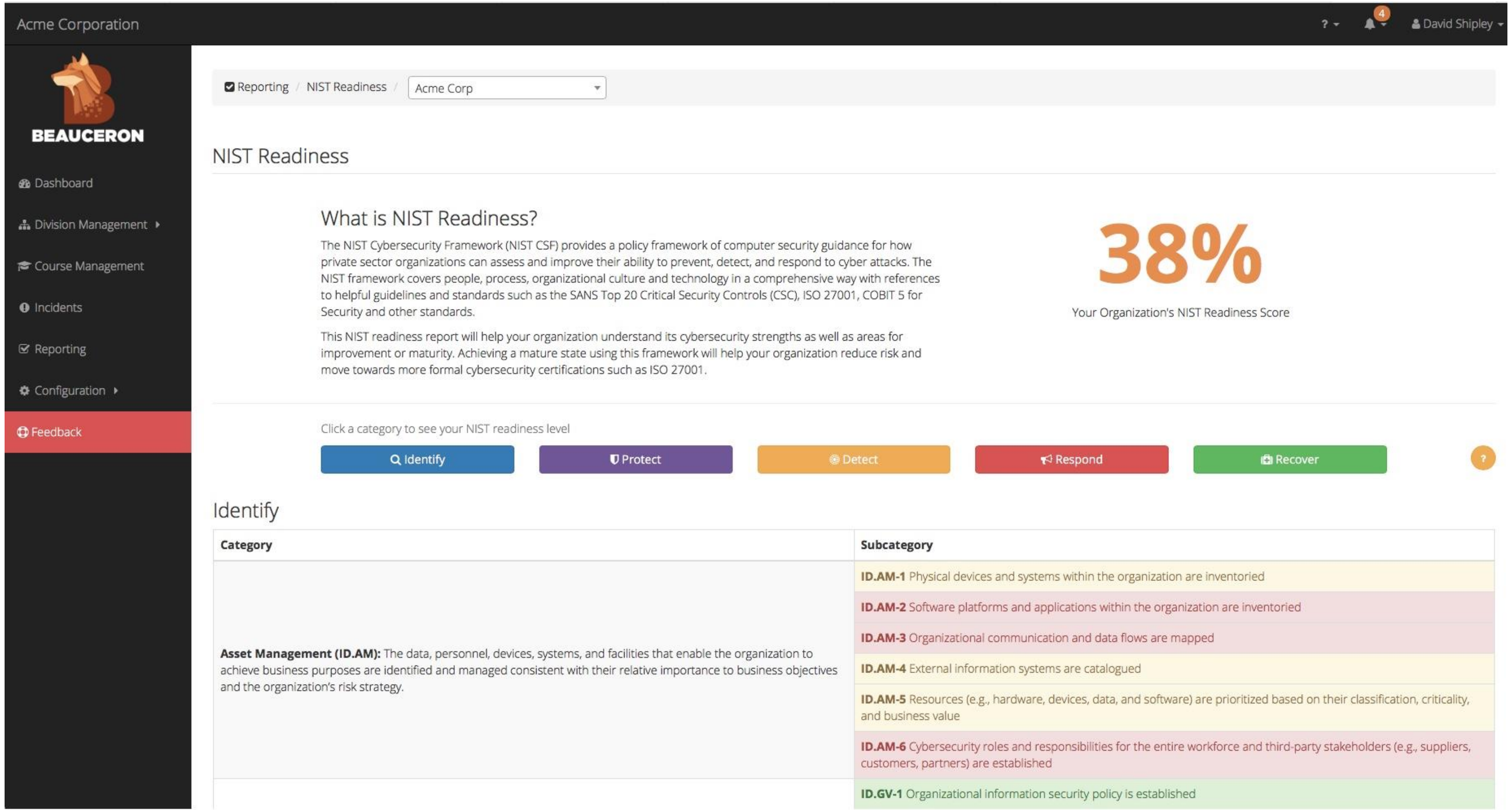
Engaging management

- Finding and measuring perceptual gaps between management, IT and organizational members
- Making cybersecurity an issue for entire organization, not just IT department
- Providing new metrics, tools to empower managers, directors, VPs and C-Suite



→ Security Dissonance Score

Tackling organizational cyber risk



NIST Readiness

What is NIST Readiness?

The NIST Cybersecurity Framework (NIST CSF) provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks. The NIST framework covers people, process, organizational culture and technology in a comprehensive way with references to helpful guidelines and standards such as the SANS Top 20 Critical Security Controls (CSC), ISO 27001, COBIT 5 for Security and other standards.

This NIST readiness report will help your organization understand its cybersecurity strengths as well as areas for improvement or maturity. Achieving a mature state using this framework will help your organization reduce risk and move towards more formal cybersecurity certifications such as ISO 27001.

38%

Your Organization's NIST Readiness Score

Click a category to see your NIST readiness level

Identify

Category	Subcategory
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1** Physical devices and systems within the organization are inventoried
	ID.AM-2 Software platforms and applications within the organization are inventoried
	ID.AM-3 Organizational communication and data flows are mapped
	ID.AM-4 External information systems are catalogued
	ID.AM-5 Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
	ID.AM-6 Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
	ID.GV-1 Organizational information security policy is established

Benefits of our approach

Awareness to Accountability and on to Agency

Insightful Dashboard and Reports

Quick and Simple to Deploy

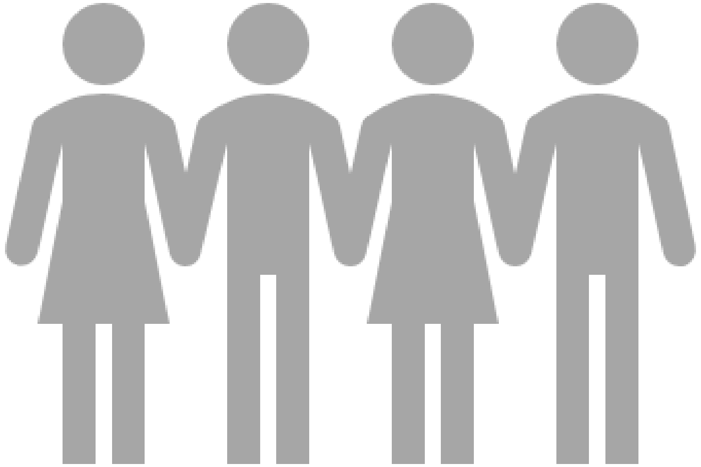
Value

- >80% say they’ve learned from the experience
- 100% confirm after completing the training they understand their role and responsibility to protect their organization
- Up to 90% reduction in phishing response rate
- 60% of security professional time freed for other projects

BEAUCERON

Beauceron Fall Insights

- 30% of users admit to storing confidential organizational information in personal cloud sites
- 38% of employees admit to using the same password for multiple accounts
- 13% of employees admit to sharing their work password with someone else because it was required for work



BEAUCERON

Key success criteria for effective awareness campaigns

- Management buy-in and commitment
- Continuous learning approach
- Use more than digital – talks, posters, newsletters can help
- Use mix of rewards and punishment

BEAUCERON

Key success criteria for effective awareness campaigns

- Well-executed events can energize the program and draw additional attention

- Effective use of compute—based training, including just-in-time learning opportunities

- Effective use of teachable moments via simulated phishing, texting, voice or USB-drop

BEAUCERON

Key success criteria for effective awareness campaigns

- Create a security portal, a one-stop shop for organizational and personal cybersecurity information

- Breakdown complex topics into short, clear, actionable steps, i.e. how to report a phish.

Why campaigns fail:

- Information provided one-time or in a way that people can not grasp (security jargon)

- Overly focused on compliance. Compliance isn’t security and security covers more than compliance.

- No or limited opportunities for continuous reinforcement / teachable moments

BEAUCERON

Why campaigns fail:

- Lack of engaging or relevant materials
- Not collecting metrics
- Unreasonable expectations
- Lack of breadth of education materials. It’s about more than phishing and passwords

BEAUCERON

BEAUCERON