LISTENING TO THE WISDOM OF THE CROWD:

WHAT OUR PEOPLE CAN TEACH US ABOUT SECURITY AWARENESS

CEO AND CO-FOUNDER, BEAUCERON SECURITY

LEAD THE SECURITY PRACTICE AT UNB

CANADIAN FORCES VETERAN

David Shipley
Beauceron Security

Our Story

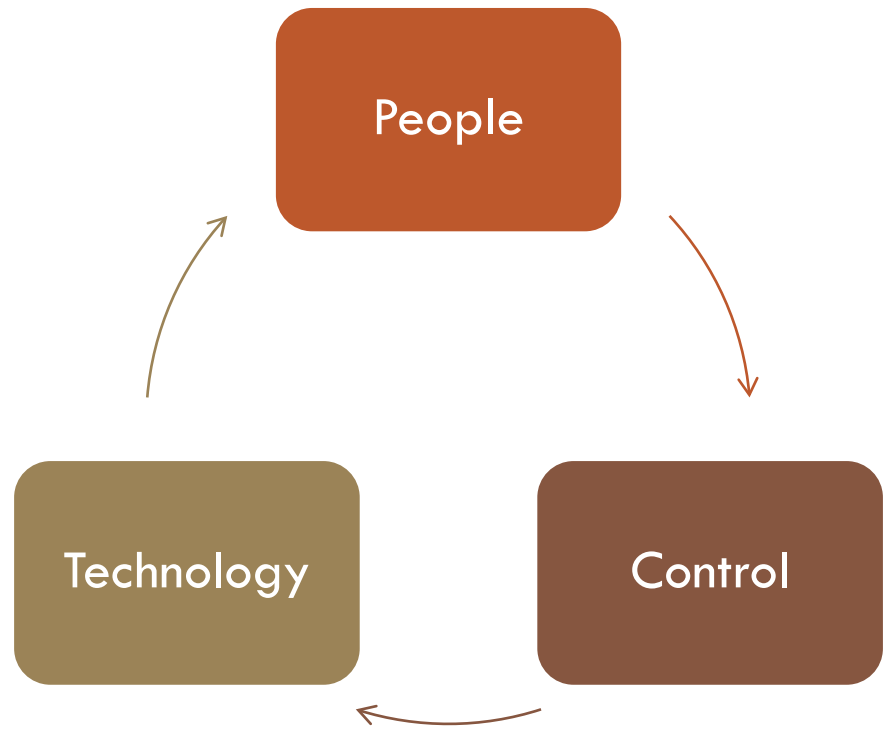Practical experience defending University of New Brunswick from 2012 to 2017.

120+ customers in 37+ countries.

Clients in retail, IT, higher education, government, manufacturing.
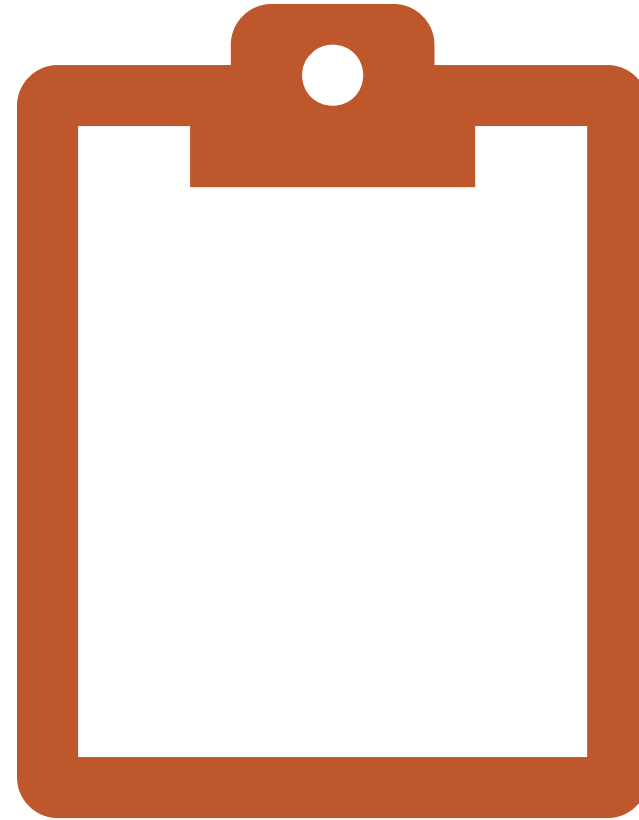
To create a better world by helping people feel empowered and in control of technology

The Meaning of *Cyber*

By the numbers: Learning from our people

The Survey

Universal user awareness, perceptions and behavior survey.

Beyond awareness – identifying the level that people care about security.

We use elements of the data to inform personal and organizational cyber risk scores.

Data is leveraged to create actionable metrics

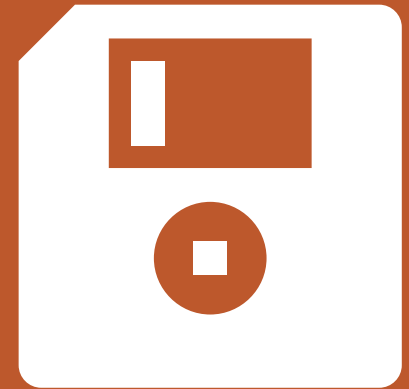# The survey in context of our approach

The Data

The following aggregate data has been compiled from a variety of industries.

Most, but not all, data is from Canadian users.

Not all users answered all questions. Sample size provided per question for context.

Totals may not add up to 100% due to rounding

Awareness - Policies

Our organization has policies on acceptable use of organizational technology and on information security.

- Yes: **94.81**%

- No: **.55**%

- I'm Not Sure: **4.64**%

Sample size: 23,466

Awareness - Role

I am aware of my responsibilities for the responsible use of organizational technologies, and my role for protecting my organization and myself from cyber attacks.

- Yes: **96.97%**
- No: **3.03%**

Sample size: 22,135

Awareness – BYOD / Remote Work

Are you aware of your responsibilities to keep your personal devices secure if you are using them to access organizational information and services?

- Yes   **90.23%**

- No   **9.77%**

Sample size: 8,467

Awareness - Phishing

Do you know what a phishing e-mail is?

- Yes: **87.65%**
- No: **12.35%**

Sample size: 23,429

Awareness - Phishing

When you receive an e-mail with an attachment, what do you do?

- Open it as long as you know the person or company.   **10.02%**

- Make sure the e-mail is from someone you know and is a file you were expecting before opening.   **89.48%**

- Always open an attachment in an e-mail to see what it is.   **0.05%**

Sample size: 23,466

Awareness - Observations

o   Awareness versus Knowledge

o   Policies don't translate into a set of instructions – i.e. how to work securely. Less about the what, more about the how and why.

o   We need to move beyond what phishing is and knowing and understanding why it's bad and how it works

Perception - Threat

Our organization is a target for cybercriminals

- Strongly agree   **36.17%**
- Agree   **46%**
- Neither agree or disagree   **15.12%**
- Disagree   **2.25%**
- Strongly disagree   **0.46%**

Sample size: 23,445

Perception – Role

I play an important role in protecting my organization from cyberattacks.

- Strongly agree   **54.93%**
- Agree   **37.58%**
- Neither agree or disagree   **6.19%**
- Disagree   **1.09%**
- Strongly disagree   **.22%**

Sample size: 22,717

Perception – Leadership

Cybersecurity is a priority for the leadership of this organization.

- Strongly agree   **55.69%**

- Agree   **36.76%**

- Neither agree or disagree   **6.19%**

- Disagree   **1.09%**

- Strongly disagree   **0.22%**

Sample size: 22,717

Perception – Cybersecurity

Cybersecurity is mostly an information technology issue.

- Strongly agree   **7.88**%

- Agree   **23.48**%

- Neither agree or disagree   **19.01**%

- Disagree   **34.83**%

- Strongly disagree   **14.85**%

Sample size: 23,431
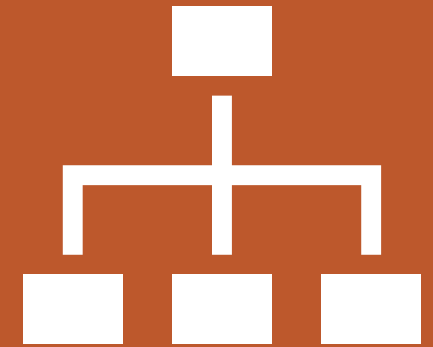
Perception – Cybersecurity

Cybersecurity is a business issue that affects the entire organization.

- Strongly agree   **62.21**%
- Agree   **33.45**%
- Neither agree or disagree   **2.96**%
- Disagree   **0.99**%
- Strongly disagree   **0.38**%

Sample size: 22,717

Perception – Education and Training

I feel that I have been provided the education and awareness necessary for me to protect myself and my organization.

- Strongly agree **22.29**%
- Agree **47.97**%
- Neither agree or disagree **20.55**%
- Disagree **7.61**%
- Strongly disagree **0.99**%

Sample size: 22,553

Perceptions - Observations

o People are aware cybersecurity is an issue for the entire business and know they play a key role

o But a third don't feel they're educated and trained enough to make a difference – and they're right

Behaviour – Phishing

Have you clicked on a link in a phishing e-mail?

- Yes, once.   14.44%
- A few times   4.9%
- Never   66.65%
- I'm not sure   14%

Sample size: 23,466

Behaviour – Reporting security concerns

I always report any potential cyber security incidents such as phishing e-mails, malware or unusual behavior on my computer(s) or device(s) to the appropriate people in my organization.

- Yes **66.54**%

- Sometimes **18.03**%

- No **7.05**%

- I'm not sure **8.37**%

Sample size: 23,441

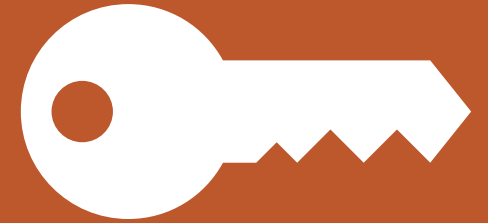# Behaviour – Work passwords

Have you shared your work password with someone else?

- Yes   **0.49**%
- Yes but it was essential for work   **6.77**%
- No   **92.59**%
- I'm not sure   **0.16**%

Sample size: 23,444

Behaviour – Password Re-use

Have you used the same password on more than one online service or website?

- Yes: **24.38%**

- Yes, but only on a few sites or services I trust: **20.57%**

- Yes, but I never re-use my work password: **25.74%**

- No, I always use unique passwords: **29.31%**

Sample size: 23,441

Behaviour – Social media

Do you regularly review (at least once a year) your privacy and security settings on your social media sites?

- Yes **64.43%**

- No **35.57%**

Sample size: 16,802

Behaviour – Downloading software

Have you downloaded and installed software from the Internet on your work computer?

- Yes **7.7**%

- Yes, it was essential for work **25.27**%

- I'm not sure **3.34**%

- No **62.38**%

- I can't (but I would if I could) **1.31**%

Sample size: 23,441

Behaviour – BYOD / Remote work

Do you use your own personal devices (such as a personal smartphone, tablet, home computer or personal laptop) to access organizational information and services?

- Yes   **36.05%**

- No   **63.95%**

Sample size: 23,438

Behaviour – Personal cloud

Do you use personal cloud services (such as Dropbox, Google Drive, or Apple iCloud) to store organizational information?

- Yes **13**%

- No **87**%

Sample size: 23,442

Behaviours – Observations

o We need to make it easier to do the right thing than it is the wrong thing.

o We need to spend more time asking questions around why users are doing risky actions.

o We need to draw the connections between inaction and risk by telling better stories.

Getting smart with metrics

What are S.M.A.R.T metrics?

- Specific
- Measurable
- Actionable
- Realistic
- Timely

Recommendations:

- Provide more specific education and training related to real attacks or attempts on your organization or industry.

  Metric: % **change in users who believe the organization is a target**

- Provide improve methods for reporting security concerns and acknowledging people for doing so.

  Metric: % **of people who report a simulated or real phish at least once in any given month, quarter or even year.**

Recommendations:

- Review why users share work passwords for work passwords. Provide improved processes and tools.

  Metric: % **change in users who report sharing work passwords**

- Provide password management tools to users.

  Metric: % **of users who say they re-use passwords**

Recommendations:

- Review risks around personal public cloud storage usage. Clarify policies, provide better tools to users.

    Metric: % **change in users who report sharing storing work information in personal cloud sites.**

- Provide social media privacy and security training.

    Metric: % **of users who say they regularly check their social media security at least once a year.**

2020 Survey

- I understand how the security tools my organization provides me help protect my information and my devices.

- Having any security tools such as firewall or antivirus mean I am completely protected from in internet threats.

- How do you manage your passwords?

2020 Survey

- In my role the information in my custody is a target for criminals.

- Cybersecurity is a priority for your manager, supervisor or leader.

- Do you send or save work information to personal e-mail accounts (Gmail, Hotmail) or store in personal drives (Google, OneDrive)?

- It's okay to take photos of whiteboards, drawings or other work information with your mobile device so you can review it later.

A Deeper Dive in Phishing

Top 10 Phishes

#10 – Apple Download Notice – 6%

#9 – LinkedIn – New Device – 6%

#8 – O365 Upgrade – 7%

#7 – Doodle Pool – 7%

#6 – Staples Order Confirmation – 7%

Top 10 Phishes

#5 – Microsoft 365 Security Alert – 8%

#4 – New Voicemail Message – 9%

#3 – Parking Ticket – 9%

#2 – Canada Post – 11%

Top Phish

Job Opportunity – 25%

Branded Versus Unbranded Phishes

Branded phishes average click rate, 1H19: **2.92**%

Unbranded phishes average click rate, 1H19: **2.93**%

Thank you

If you'd like a copy of the questions and survey data, please chat with me.

Appreciate any ideas on how we could improve our surveys to deliver more value to the community.

If you'd like to stay informed on our Canadian phishing simulation data, please talk to our team about subscribing to our newsletter.