SEPTEMBER 30, 2021

National Day of Truth & Reconciliation

LAND ACKNOWLEDGEMENT

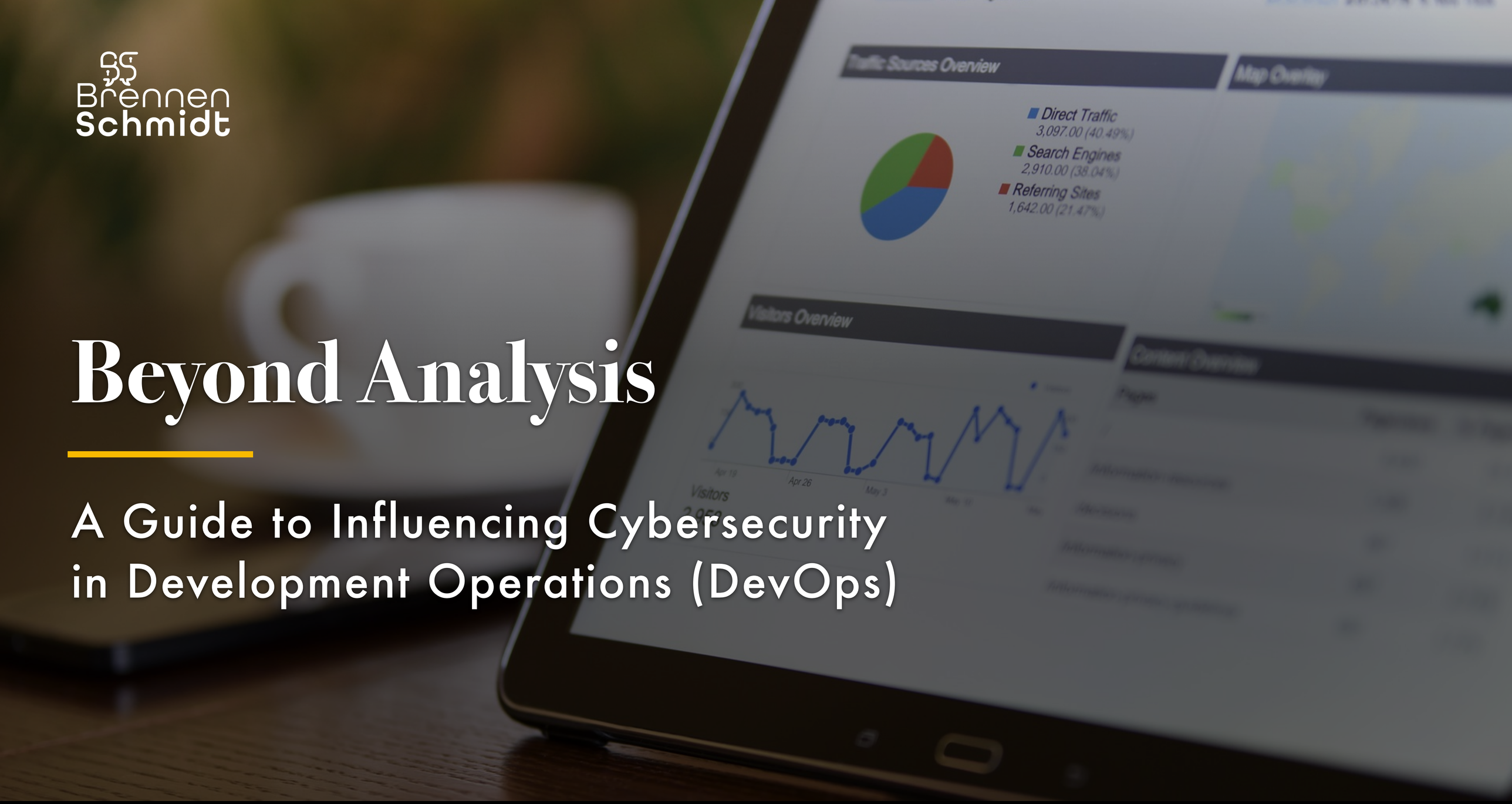
We would like to acknowledge that we are on the traditional lands, referred to as Treaty 4 Territory, and that the city of Regina is located on Treaty 4 territory, the original lands of the Cree, Ojibwe (OJIB-WĒ), Saulteaux (SO-TO), Dakota, Nakota, Lakota, and on the homeland of the Métis Nation.

We respect and honour the Treaties that were made on all territories, we acknowledge the harms and mistakes of the past, and we are committed to move forward in partnership with Indigenous Nations in the spirit of reconciliation and collaboration.

Brennen Schmidt

Beyond Analysis

A Guide to Influencing Cybersecurity in Development Operations (DevOps)



ABOUT ME

Brennen Schmidt (he / him)

BEd, PR (Cert.), UXC, CUA

THOUGHT LEADER & SPEAKER

Co-author: *Cyber City Safe: Emergency Planning Beyond the Maginot Line*

PROFESSIONAL EXPERIENCE

- Summer Student — Government of Saskatchewan
- Communications Consultant — Government of Saskatchewan
- Communications Specialist — eHealth Saskatchewan
- Consultant — Deloitte.
- Senior Consultant — Deloitte.

NATIONAL & LOCAL CYBERSECURITY COMMENTARY

CBC SASKATCHEWAN · Global REGINA · CTV NEWS CHANNEL · CTV NEWS REGINA · NEWS TALK 980 CJME · CANADA TALKS · NP RADIO

INTRO

What Brought Us Here?

QUOTE

“There seems to be a disconnect…”

- Professional Jargon

PROBLEM

Development & Operations: Art Imitating Life?

Draw On My Back Challenge: Brooke and Jeffrey (YouTube)

PROBLEM

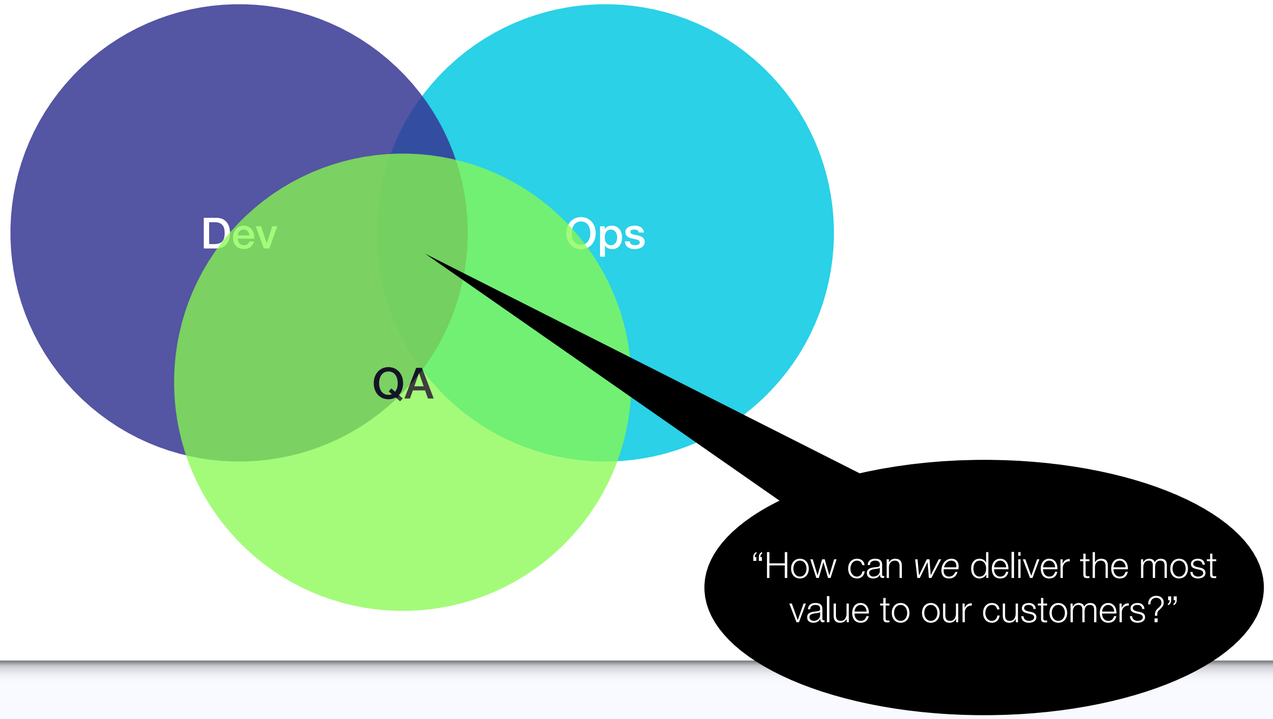
We've Established "Stove Pipes" within Organizations

Development and validation is split up for "someone" in ops to look after...

SOLUTION

We Can Promote Value Delivery using DevOps

Exercise a “customer obsessed" mindset to better meet business objectives with agility.



CRAWL

DevOps: A Better Way

PROBLEM

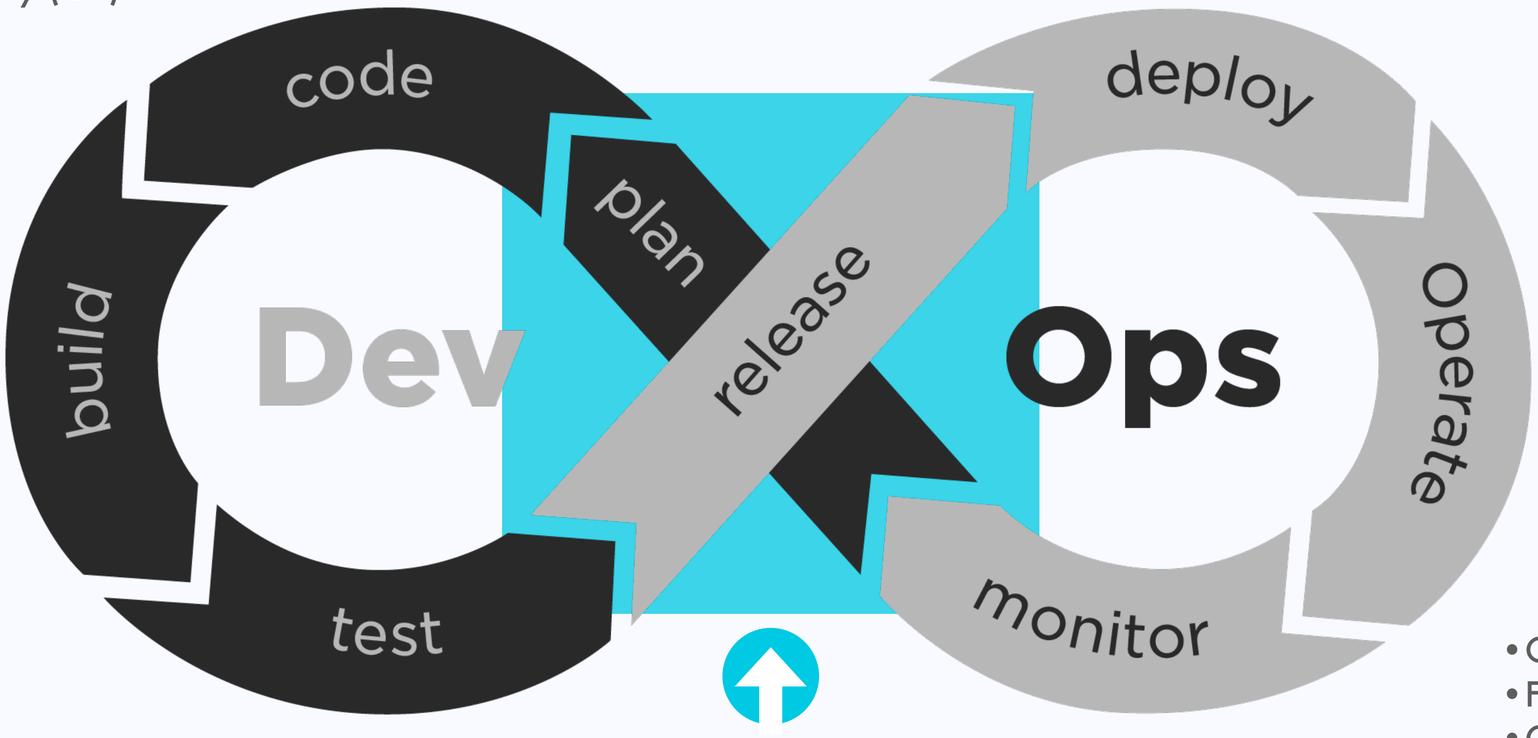
Help Prevent the "Cheeto Lock" of Cybersecurity Today

Source: Know Your Meme

SOLUTION

Explore the Introduction of the DevOps Workflow

- Continuous Integration (CI)
- Continuous Delivery (CD)
- Version Control
- Release Control



- Cross-Functional Collaboration
- Feature Management
- Continuous Improvement
- Solution Communication

Source: DevOps Workflow (Pease, 2017)

WALK

The DevSecOps Journey

NOTE

Hacking is Not a Crime

Embrace and leverage security researchers to become more secure

SAFETY

Decrease Risk with an Outside Perspective

Exploring collaboration opportunities with researchers through bug bounty programs can help decrease vulnerabilities in the Software Development Lifecycle (SDLC).

76%

of apps have at least one security flaw

24%

security flaws identified as high-severity

~66%

have more security findings in 3rd party code

RESOURCE  https://www.veracode.com/state-of-software-security-report

Source: Veracode State of Security Today vii (2021)

TECH

Put Theory into Practice with Design and Secure Coding

The Open Web Application Security Project (OWASP) framework is a starting point.

Define Security Requirements	Ensure security is implemented through the development process
Leverage Security Frameworks & Libraries	Define security capabilities to make securing applications easier
Secure Database Access	Prevent injection attacks by pre-building SQL queries and configure secure database access
Encode and Escape Data	Remove the ability for a user or automation to include special characters
Validate All Inputs	Maintain a “zero trust” mindset; trade user input as being untrusted and / or filter
Implement Digital Identity	Enable Multi-Factor Authentication (MFA), secure passwords (and recovery), and secure sessions
Enforce Access Controls	Deny by default; apply principle of least privilege; conduct routine checks of access control(s)
Protect Data Everywhere	Leverage encryption while data is in transit and at rest

RESOURCE **OWASP Framework**

Source: CompTIA Security+ 601 Study Guide, *Designing and Coding for Security* (p. 139)

BUSINESS

When You Think Cyber, Think CIA

Leverage CISA's of "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring [CIA] of information"

Confidentiality

Keeping data or information private or secret.

Integrity

Quality or completeness of information; it can be trusted.

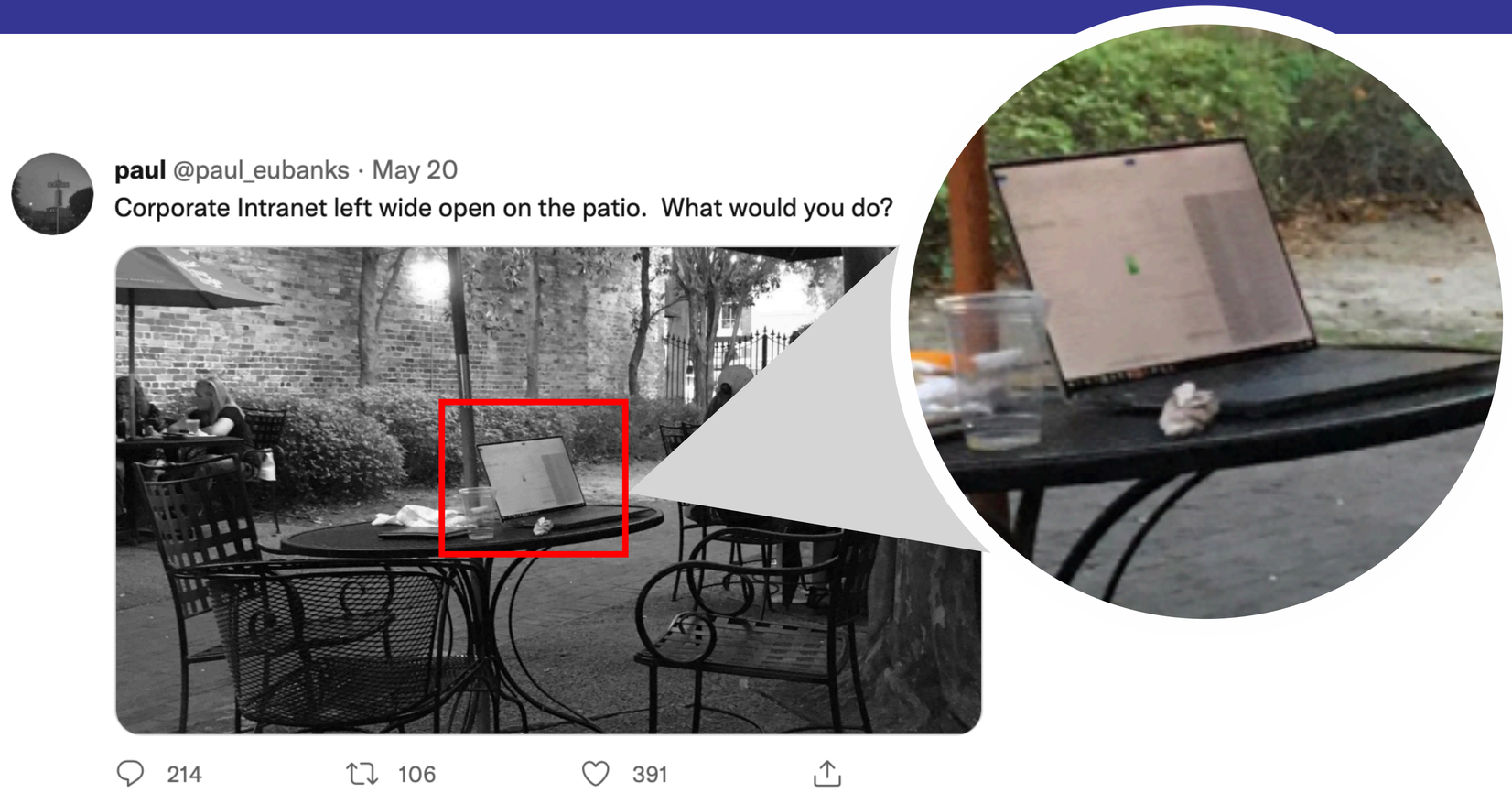
Availability

Authorized users have timely access to resources.

Source: Cybersecurity & Infrastructure Security Agency (CISA)

REMEMBER

Put Yourself in Your Customer's Shoes



Source: Twitter

START

Craft the Story for a Safer Future, for Everyone

Alyssa Miller 👑 Duchess of Hackington ✔
@AlyssaM_InfoSec

It's so important to not over think threat modeling, to get it done early in the pipeline, to do 8t 8n manageable chunks, and to give the business a voice!! @WiCySorg #WiCyS2021

> **Maggie Marxen** @MaggieMarxen · 2021-09-09
> Learned so much today from @AlyssaM_InfoSec!
> A standard user story: “As a _____ I want to _____ so that _____”
> A DevSecOps user story: “As a _____ I want you to protect _____ from _____” #WiCyS2021 @WiCySorg

5:03 PM · 2021-09-09 · Twitter for Android

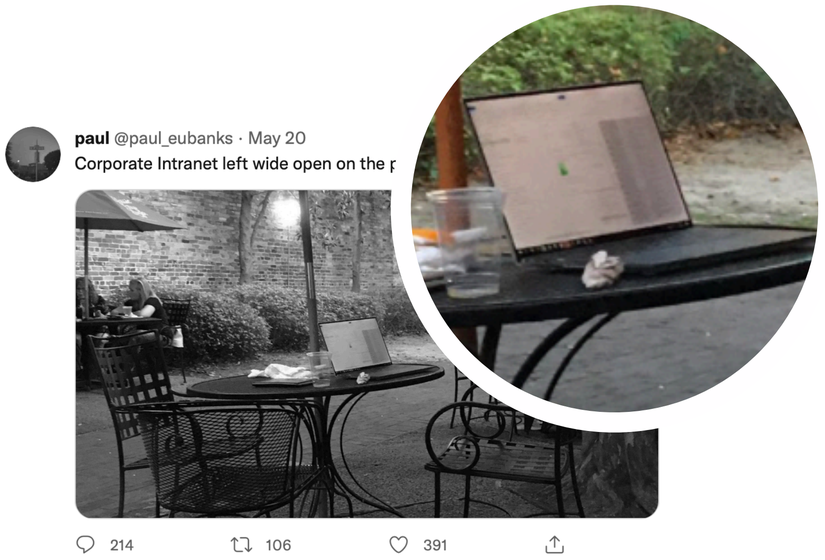
7 Retweets **29** Likes

Source: Twitter

BUSINESS

Example: Protecting Our Users at the Coffee Shop

Connect the dots among and between stakeholders by re-framing your user stories; by doing so, you can help team members empathize with personas.



> As a [business analyst], I want to protect [mobile users] from [someone accessing their device if they leave it unattended for a period of time].

User Story adapted from: Alyssa Miller (@alyssam_infosec)

RUN

Codify Your Future 

REMEMBER

“Use each word like a precision instrument.”

Ted Sorensen

FORECAST

A Shared Focus on Precision in Documentation and Code

Infrastructure-as-Code (IaC)

```
"resources": [
    {
      "type": "Microsoft.Storage/storageAccounts",
      "name": "[variables('storageAccountName')]",
      "location": "[parameters('location')]",
      "apiVersion": "2018-07-01",
      "sku": {
        "name": "[parameters('storageAccountType')]"
      },
      "kind": "StorageV2",
      "properties": {}
    }
  ],
```

Microsoft Azure Resource Manager (ARM) JSON Sample

Policy-as-Code (PaC)

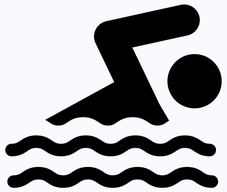
```
import "time"

# Validate time is between 8 AM and 4 PM
valid_time = rule { time.now.hour >= 8 and time.now

# Validate day is M - Th
valid_day = rule {
  time.now.weekday_name in ["Monday", "Tuesday", "W
}

main = rule { valid_time and valid_day }
```

HashiCorp Sentinel Policy Language Sample

Source: Microsoft (ARM Template Example) | Hashicorp Sentinel (Policy Example)

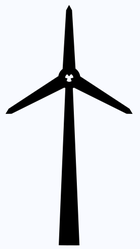
SAFETY

Communicating Cybersecurity Means the World to Us…



Water Security

Food Security



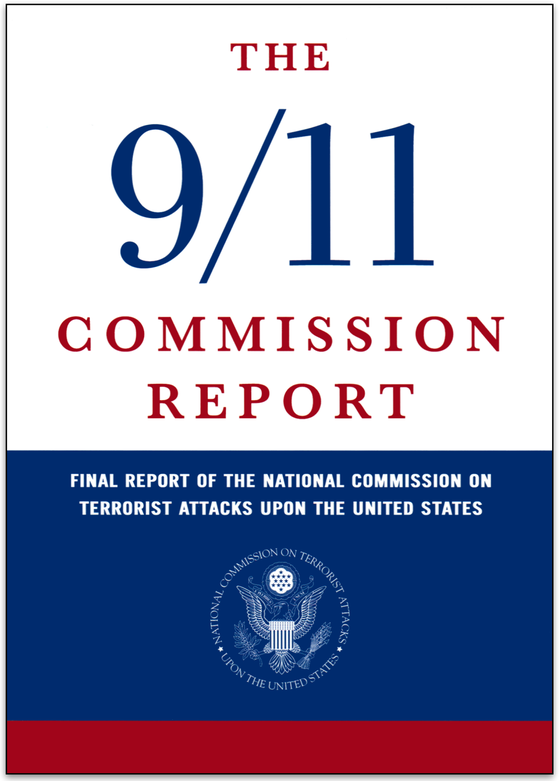
Energy Security

Public Health Security

Source: Brennen Schmidt

SAFETY

Exercise Imagination to Build Resiliency



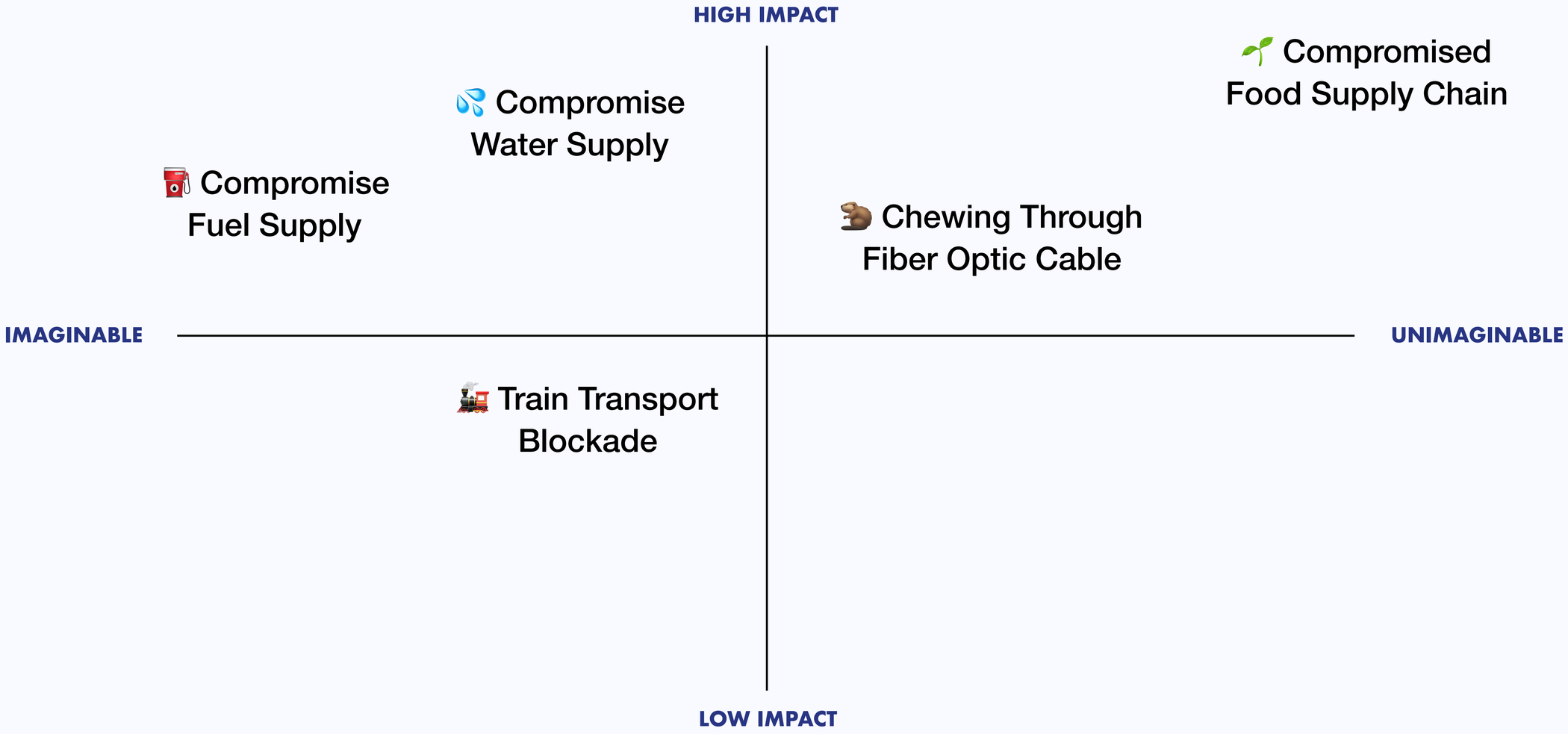
"**Imagination is not a gift usually associated with bureaucracies.**"

"It is therefore crucial to **find a way of routinizing, even bureaucratizing, the exercise of imagination**. Doing so requires more than an expert who can imagine that aircraft could be used as weapons. Indeed, since Al Qaeda...had already used suicide vehicles...the leap to [use] other vehicles...is not far-fetched."

Source: The 9/11 Commission Report (2004), page 344

SAFETY

Be the Voice to Help Thwart Actions Beyond Imagination



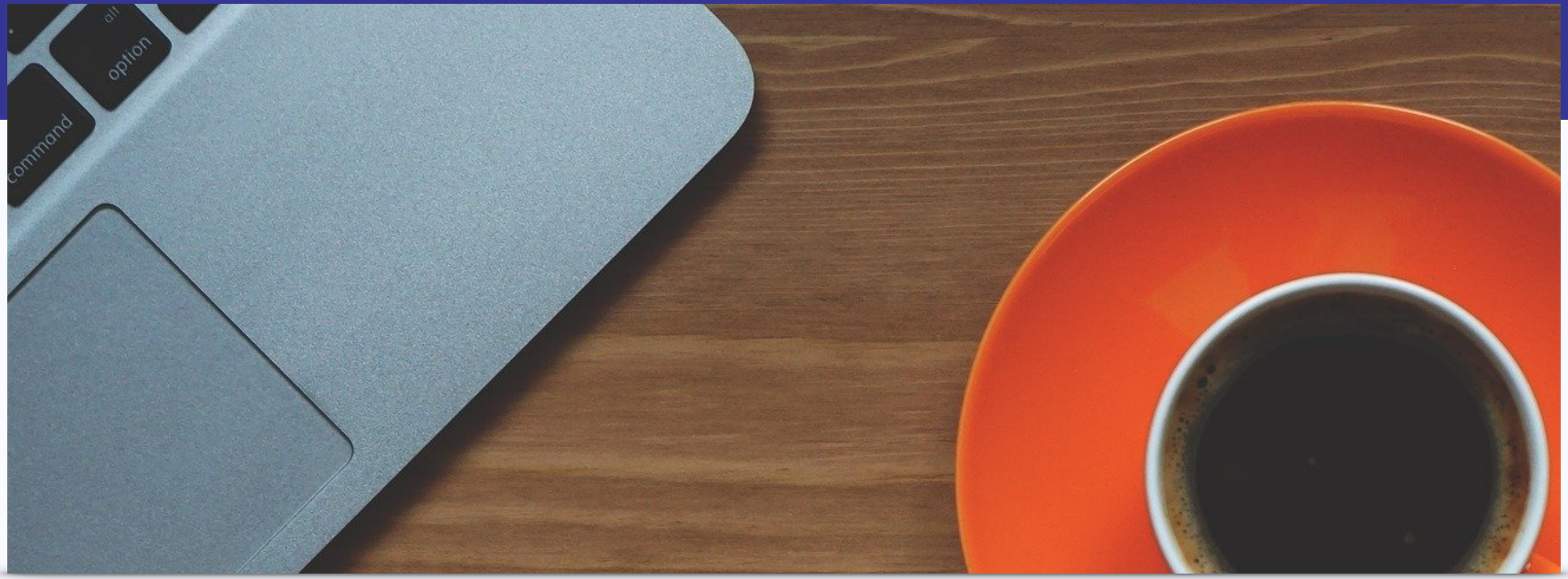
Source: Brennen Schmidt

Now is your opportunity to decode security…

Source: Pixabay

ACTION

Commit to Having a #CyberCoffeeChat



Source:Pixabay

TO-DO

Lead these 10 Key Steps in the Next 30 days

1. Determine who is responsible for managing your primary domain name, then check to see what security measures are in place to maintain its security
2. Maintain a running list of all official (and unofficial) names of digital properties under the ownership of your organization
3. Remove brand identity guidelines posted on the public internet. Should external users or agencies require this information, deliver it to them in a secure (encrypted) format
4. Complete an inventory of users, applications, and third parties that are capable of accessing digital services on your organization's behalf. Remove or limit as appropriate
5. Phase out the distribution of corporate-branded hardware items, including USB devices; it's not worth the risk to your organization's reputation
6. Complete an inventory of your online services, including social media and cloud services
7. Reach out to team members representing IT, security, privacy and legal to engage in the conversation to help identify risks and how to mitigate them
8. Research the availability of account recovery processes for identified online services
9. Document any available account recovery process for each identified service; record on paper and store the key(s) provided in a safe place
10. Encourage users not to click on that phishing email offering a free coupon at a coffee shop – it's safer to just to pay!

THANK YOU

Let’s connect

brennenschmidt.ca

Twitter: @brenzens

Disclaimer

This presentation is not, and should not be construed as advice of any kind on participants' stance on cyber security or any other security matters. Personal and corporate decisions on all security matters are the responsibility of the person and the corporation, subject to applicable laws.

The contents of this presentation are intended for informational and educational purposes only and do not replace independent professional judgment. The author has no proprietary knowledge of participants' situations and thus assumes no responsibility for the applicability of the information presented.

Moreover, given the speed at which cyber security issues and law evolve, and given that cloud computing and other activities could be deemed to be almost anywhere, there is also no suggestion that the material in this presentation is complete, or completely up-to-date.