TOP 10 CYBERSECURITY STRATEGIES FOR SMALL BUSINESSES

Presented by:

Nick Holcomb & Kevin A. McGrail

June 23, 2021

FOR TODAY'S SESSION

- Webinar will be recorded
- All attendees will be placed on mute
- Questions may be input into the Questions Box within GoToWebinar
- We will answer questions in the final 10 minutes

MEET THE PRESENTERS

KEVIN A. MCGRAIL

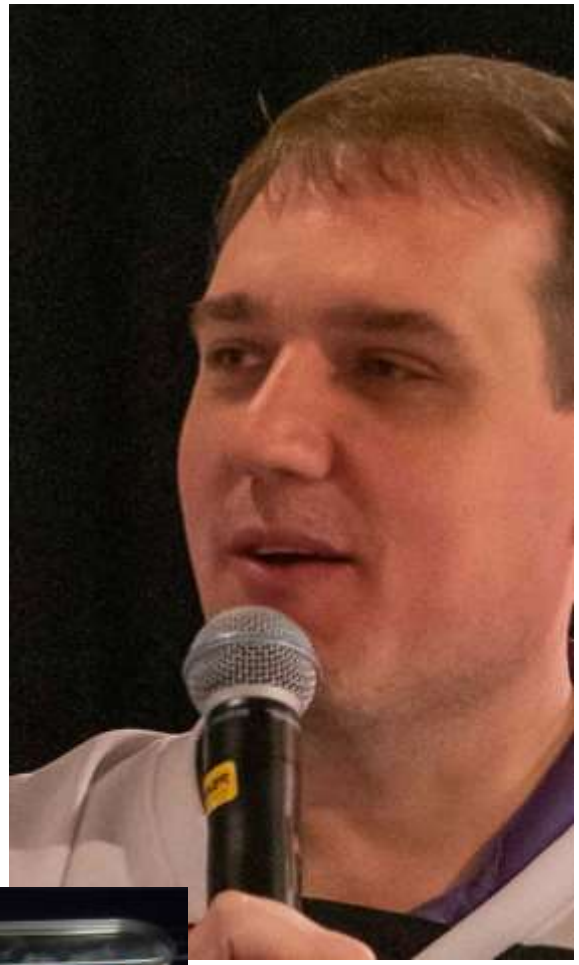
Principal Evangelist, DitoWeb.com

- Apache Software Foundation Member
- Google Workspace Top Contributor, Developer Expert & Ambassador
- U.S. Marine Corps Cyber Auxiliary Member

NICK HOLCOMB

Chief Technology Officer, Payroll Network

- 20 Years of Technology Experience
- 15 Years Industry Experience - Payroll | Talent | Time | HR Compliance | Reporting | Application Integration | Mobile | Leadership
- Microsoft Certified Professional
- B.A. American University



Nick Holcomb, CTO, Payroll Network

1 – MAKE CYBERSECURITY PART OF RISK MANAGEMENT / GOVERNANCE

- How are you approaching risk management?
  - Compliance?
  - Cyber security?

- Visit and / or Create the plans.

2 - DON'T LET PERFECTION GET IN THE WAY OF PROGRESS

START BY ANALYZING THE CYBER ISSUES THAT HAVE HAPPENED AT YOUR FIRM IN THE LAST YEAR. THEN THE LAST TWO YEARS AND SO ON.

1. Phishing attacks? Help it with phishing training.
2. Lost phone/laptop/tablet/etc.? Start Incident Response Plans.
3. Don't focus on topical or 100 year threats. No FUD!

#3 – SET UP A BUDGET FOR CYBERSECURITY

DO YOU HAVE A CYBER BUDGET?

IDEA:

USE A PERCENT OF YOUR IT BUDGET.

DON'T HAVE AN IT BUDGET, HOW DEPENDENT ON IT ARE YOU?

WHAT IS PAYROLL NETWORK'S CYBER SECURITY BUDGET?

#4 – Perform a Disaster Recovery Exercise

Exercises like: What happens if a storm hits? Uri

What happens if a power outage occurs?

What happens if hackers encrypt your data?

What happens if you lose a critical member of your team?

Bus Factor / Payroll.

Don't plan for 100-year items like the pandemic.

How does Payroll Networks Handle this?

Dito Storm Uri Roses & Thorns

#5 – UTILIZE APPROPRIATE RESOURCES

- Staff Appropriately: 55 points per IT person – 1 point / desktop, 5 / server, 4 / VM
- Use Anti-Malware, Anti-Spam, & Anti-Phishing technologies and firms
- Patch your Systems, Backup your Systems, Document your Processes, etc.
- National Cybersecurity Assessments and Technical Services https://us-cert.cisa.gov/resources/ncats

Payroll Network℠

#6 – BACKUPS, BACKUPS, BACKUPS!

- **Cold and Hot backups are the solution to Ransomware**
- **Paying ransoms could be a big issue with CFIUS/ATA/OFAC[1] and Primary & Secondary Liability**
- **Test your Backups. Backups are important, Restores are critical.**
- **Lindbergh Kidnapping and Phishing**

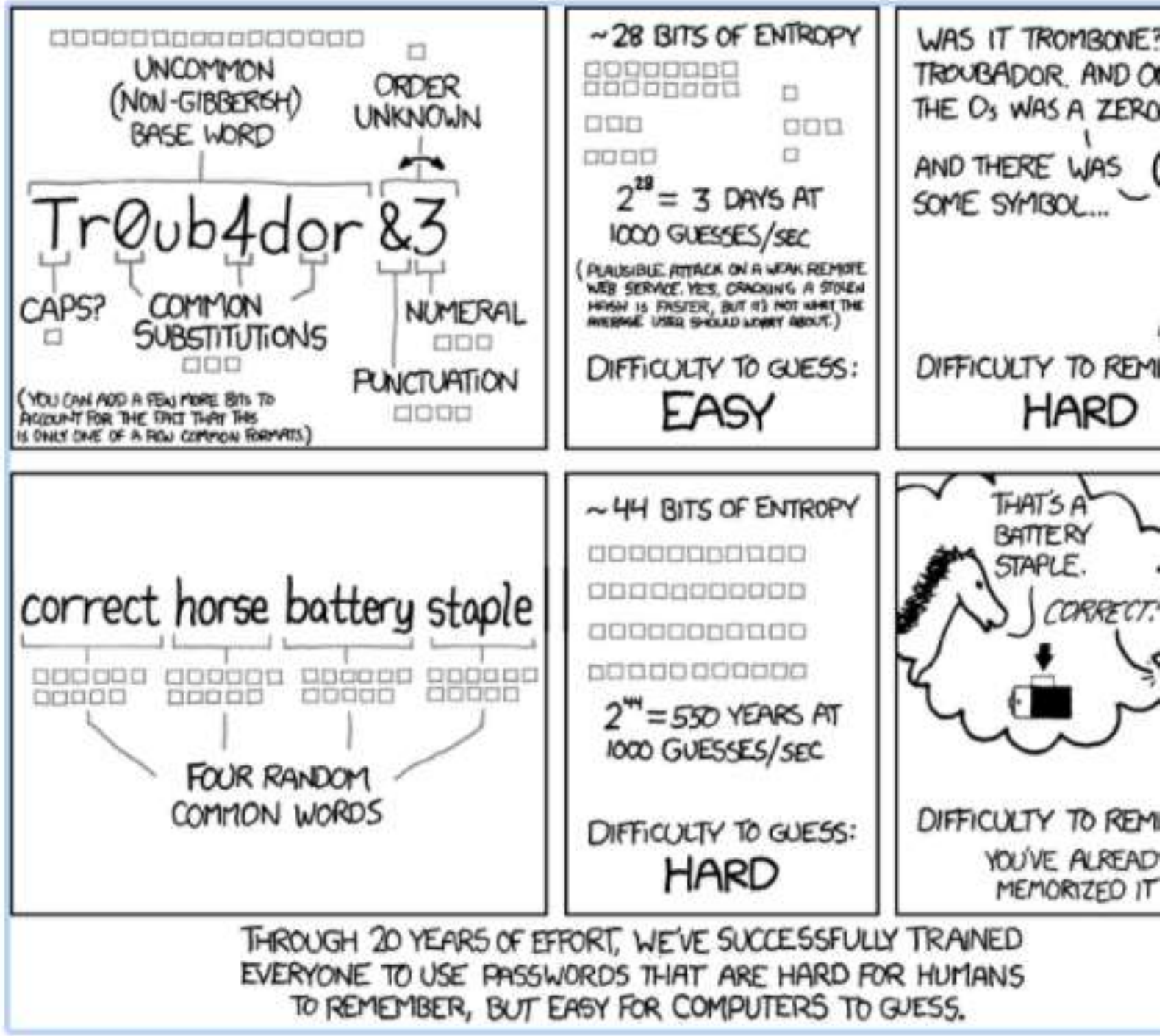
[1]https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

#7 – UPDATE YOUR PASSWORD POLICY

- Use Multifactor Authentication.
- Use Passphrases. Xkcd
- Routine changing of passwords is LESS secure.

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

WHEN'S YOUR ANNIVERSARY?



#8 – USE GOOGLE & LEVERAGE THE CLOUD

Better cyber posture than you can do alone

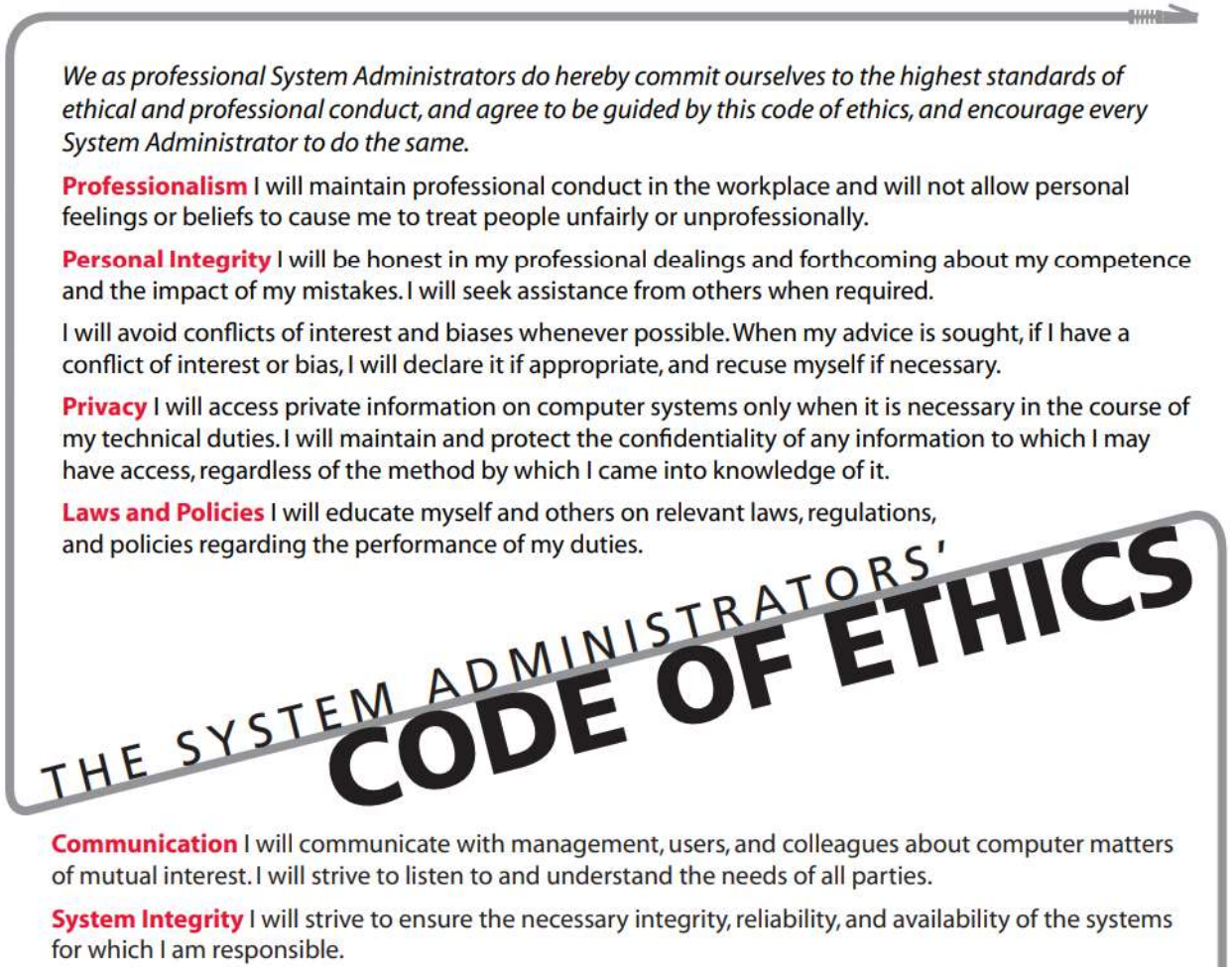
BigQuery is amazing & can analyze lots of data

Chromebooks are inexpensive & highly secure

#9 – BUILD A CULTURE OF CYBERSECURITY

- Create a culture of transparency
- Understand the psychology of scams (Separate emotion from logic)
- No passive-aggressive IT people
- Supportive Leadership
- "Built-in, not Bolted On"

#10 – ADHERE TO A CODE OF ETHICS



We as professional System Administrators do hereby commit ourselves to the highest standards of ethical and professional conduct, and agree to be guided by this code of ethics, and encourage every System Administrator to do the same.

Professionalism I will maintain professional conduct in the workplace and will not allow personal feelings or beliefs to cause me to treat people unfairly or unprofessionally.

Personal Integrity I will be honest in my professional dealings and forthcoming about my competence and the impact of my mistakes. I will seek assistance from others when required.

I will avoid conflicts of interest and biases whenever possible. When my advice is sought, if I have a conflict of interest or bias, I will declare it if appropriate, and recuse myself if necessary.

Privacy I will access private information on computer systems only when it is necessary in the course of my technical duties. I will maintain and protect the confidentiality of any information to which I may have access, regardless of the method by which I came into knowledge of it.

Laws and Policies I will educate myself and others on relevant laws, regulations, and policies regarding the performance of my duties.

THE SYSTEM ADMINISTRATORS' CODE OF ETHICS

Communication I will communicate with management, users, and colleagues about computer matters of mutual interest. I will strive to listen to and understand the needs of all parties.

System Integrity I will strive to ensure the necessary integrity, reliability, and availability of the systems for which I am responsible.

USENIX/SAGE CODE OF ETHICS

Next Steps

START THE JOURNEY TODAY!

Remember: Cyber is NEVER "done".

Processes and procedures will almost always steer you correctly in sticky situations.

Money handlers are a big target. Attacks on payroll are nothing new. Experience and controls protect you!

Payroll Network and Dito can help!

CONTACT US!

Nick Holcomb, CTO, Payroll Network
https://linkedin.com/in/nicholas-holcomb

KAM, Principal Evangelist, Dito
https://linkedin.com/in/kmcgrail