AMERICAN STRUCTUREPOINT INC.

IT SOLUTIONS

PREVENTING CRACKS IN YOUR TECHNOLOGY FOUNDATION

REALLY?

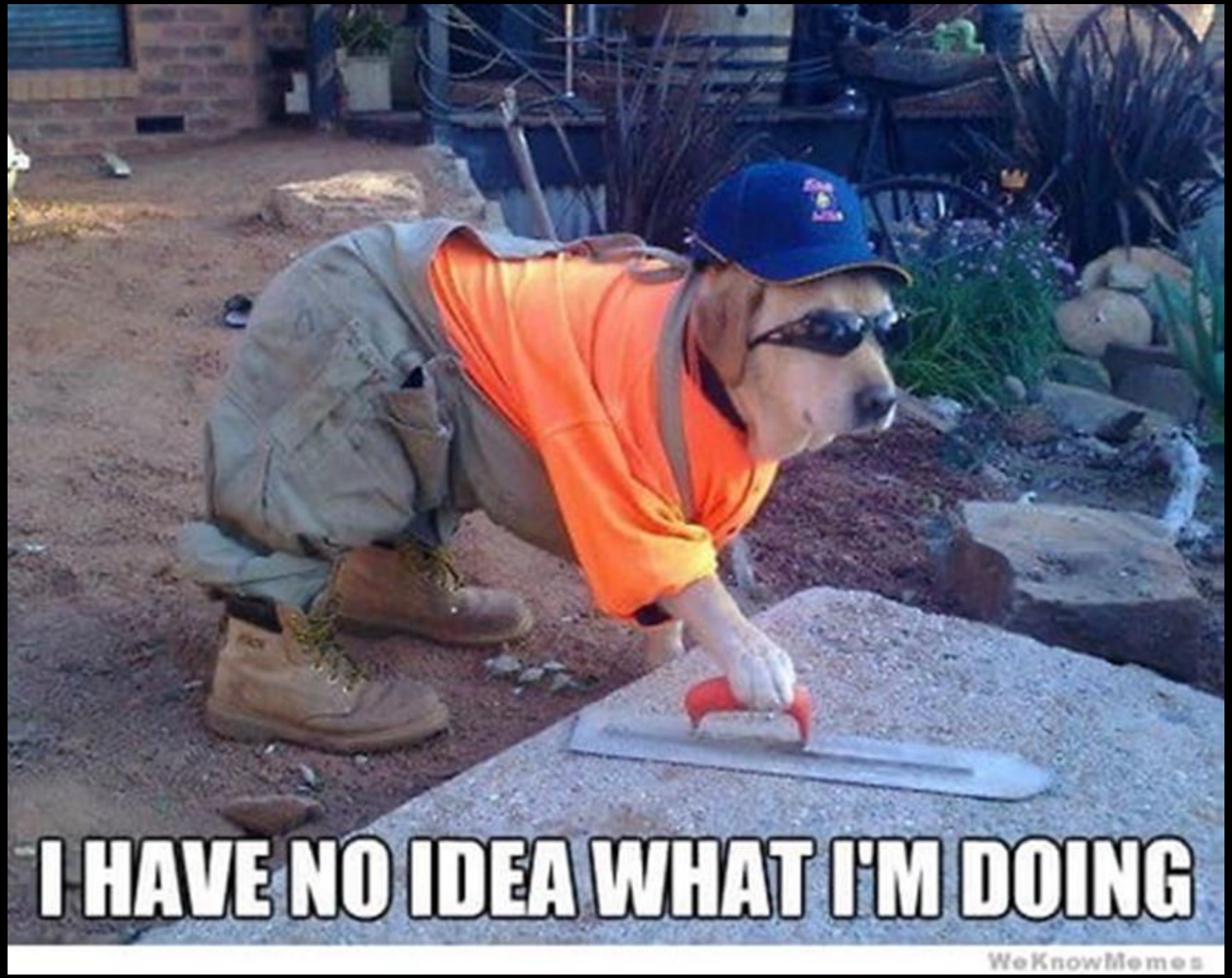
WET CONCRETE

It's like fly paper for bad drivers

auto-fail.com

FUTILITY

Some situations are just outside your capabilities unless your Clark Kent.


I HAVE NO IDEA WHAT I'M DOING
WeKnowMemes

AMERICAN STRUCTUREPOINT INC.

IT SOLUTIONS

AGENDA

INTRODUCTION & APPROACH

LATEST CYBERSECURITY NEWS

DO “HACKERS” CARE ABOUT CONCRETE?

COMMON MISTAKES AND MISCONCEPTIONS

KNOWLEDGE IS POWER – BASIC PRINCIPLES AND RECOMMENDATIONS

SIMPLIFYING YOUR STRATEGY

WHERE TO TURN

FINAL TIPS & TAKEAWAYS

ED VALASEK

AMERICAN STRUCTUREPOINT INC.
IT SOLUTIONS

IT Security Director for American Structurepoint, Inc. – A&E Firm (Indianapolis, IN)

Previous:

CIO – Financial Institution

Senior IT Consultant / Engineer

Global IT Operations Manager – Manufacturing

13-year Law Enforcement Veteran

CISSP / CCUE

InfraGard Indianapolis, IN Member

Indiana CIO Network Member

DO “HACKERS” CARE ABOUT CONCRETE?

ACCORDING TO RESEARCH:

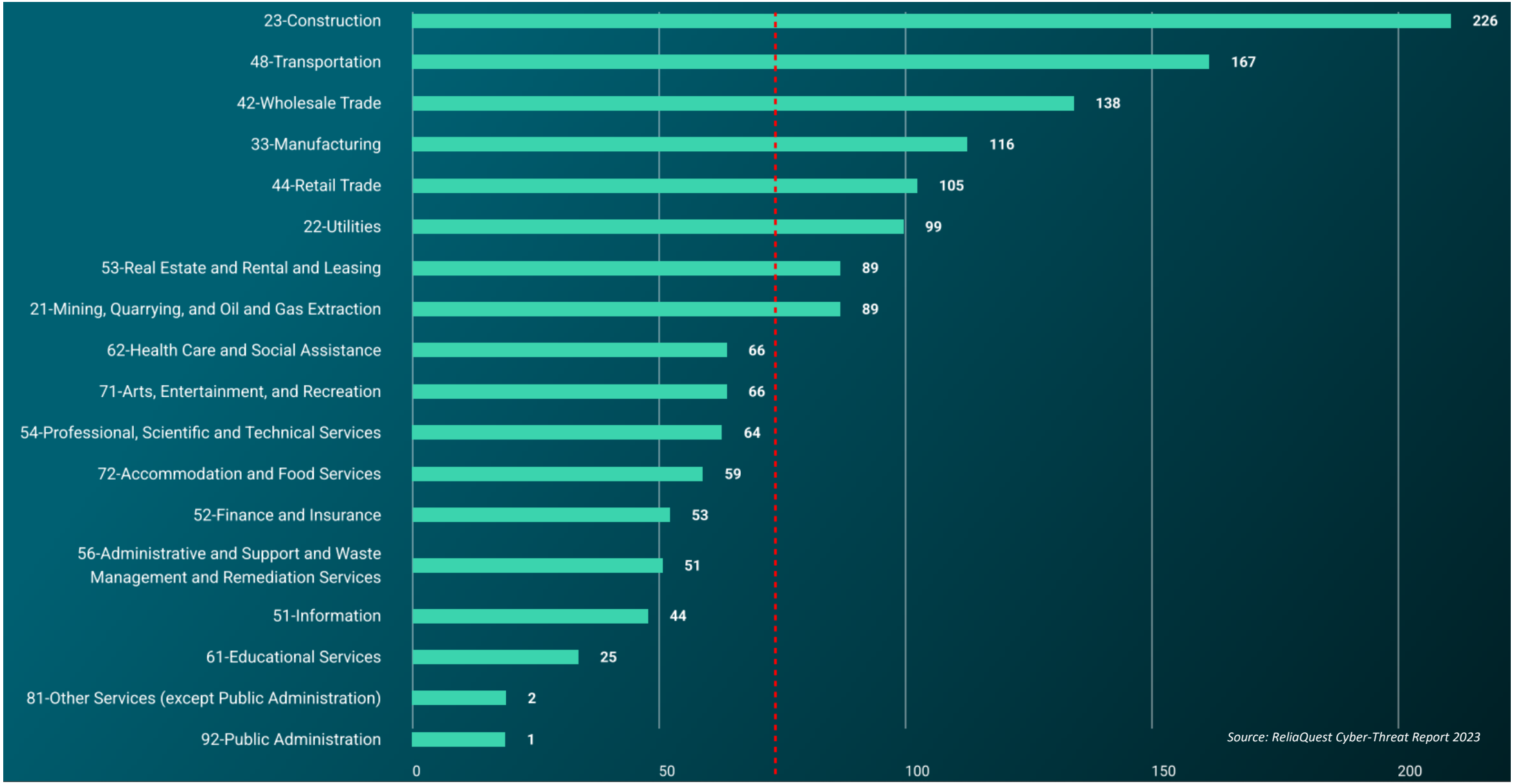
On average, it can be up to 11 days before an attacker is detected in a compromised environment. During this time they are collecting intelligence, stealing information, setting up other accounts to regain access and more…. Typically, the final step is deploying malicious software such as ransomware.

THE CONSTRUCTION INDUSTRY

A lot of businesses do not believe they need to be worried about hackers and cybersecurity. Unfortunately, the construction industry has a reputation for falling behind when it comes to security maturity and user education regarding current threats. “Threat actors” assume this and pay attention to this information. It’s their job, and a very lucrative one….

Why do you think the construction industry has this reputation?

TRENDS BY INDUSTRY



EXAMPLES

- Construction firm in Canada breached – Held lots of government project information and critical infrastructure information.
- California-based concrete contractor, reported an unauthorized third party was able to temporarily access its systems and files.
- Oklahoma City-based oil and natural gas company, reported a data security breach.
- Cybercriminals attempted to compromise water treatment plant networks through **industrial control systems** to poison the water supply in Florida.
- The Texas Department of Information Resources (DIR) is leading the response to a ransomware attack against entities across Texas - 2019.

COMMON MISCONCEPTIONS ABOUT CYBERSECURITY

1. Basic cybersecurity training is good enough
2. All security products are adequate
3. The “cloud” solves my security concerns
4. Cybersecurity is IT’s responsibility
5. ‘More’ cybersecurity is ‘Better’
6. Strong passwords provide adequate security
7. Security tools and technologies are protection enough
8. Multi-factor authentication is not vulnerable to compromise
9. No one wants our information, won’t happen to our company
10. Cybersecurity is “one and done”
11. Security through obscurity is a strategy
12. Cybersecurity is too complicated for my business
13. Cybersecurity is too expensive

KNOWLEDGE IS POWER

BASIC PRINCIPALS

The NIST CIA triad is a model that helps organizations implement information security programs to protect their confidential and sensitive data.

Typically, this is carried out through policies, processes, and procedures.

- **Confidentiality:** Access to information should be restricted to only those who need it.

- **Integrity:** Information should be accurate, reliable, and protected from unauthorized modification, destruction, and loss.

- **Availability:** Authorized persons should be guaranteed access to information when necessary.

KNOWLEDGE IS POWER

BASIC RECOMMENDATIONS

1. Back up your data **reliably**
2. Know your legal obligations
3. Grant limited access rights
4. Provide training to employees
5. User multi-factor authentication
6. Use next-generation endpoint security software
7. Update and patch software and systems regularly – **Not just Windows Operating Systems**
8. Protect all devices equally, not just PCs – Tablets, Phones, etc.
9. Implement email security
10. Manage mobile devices
11. Secure Wi-Fi
12. Establish policies
13. Buy cyber insurance
14. Implement Incident Response Plan
15. Test your systems, backups and response
16. Do not continue using end-of-life technology

KNOWLEDGE IS POWER
BASIC PERSONAL RECOMMENDATIONS

- Use strong passwords
- Change passwords frequently
- Do not open suspicious emails
- Avoid downloads from unknown sources
- Refrain clicking links in social media platforms or random text messages
- Use security protection software on all of your devices
- **Educate one another**

SIMPLIFYING YOUR STRATEGY

Key Point:

Cybersecurity is a marathon not a sprint… Trying to tackle everything at once is messy and will cause disruptions. Be diligent and committed, but at a reasonable pace you can handle.

You have a business to run, right?

SIMPLIFYING YOUR STRATEGY
GENERAL STEPS

1. Assess Your Current Security Landscape
2. Define Security Objectives and Requirements
3. Develop a Risk Management Plan
4. Develop Policies and Procedures
5. Implement Best Practice Security Controls
6. Adopt Employee Security Awareness Training
7. Continually Monitor, Test, and Improve

WHERE TO TURN

1. Many third-party providers exist that can get you on track.
2. Search on the Internet about security and the companies you do business with. What you find may surprise you.
3. Lots of great cybersecurity resources exist from NIST and other Cyber Security Framework sources.
4. Business journals and publications are now featuring security related articles. Take a moment to read them.
5. If you don’t have the time, resources, or capacity to tackle all of this as a company or yourself, **please ask for help.**

FINAL TIPS & TAKEAWAYS

- Starting with the most basic, built-in security capabilities and best practices (technical and non-technical) can take you far without having to purchase several expensive products and/or services.
- Do your homework on who you are doing business with and ask questions. Follow your instincts…
- Review your contracts – Cyber liability clauses are becoming more and more common in the private and public sector. Should you include your own?
- Are you sharing data or establishing connectivity outside of your organization?
- Start addressing High Risk, Low Effort initiatives to tackle as a starting point.
- Allow cybersecurity to be part of your overall strategic goals / plans.
- Evaluate and ask questions regarding the technologies you have and the staff or third-party managing your technology.
- Reflect on any “issues” in your environment such as recurring downtime, unreliable availability, or regular outages impacting your business. These can be indicators.
- Do not try to tackle everything yourself and ask for help. Do not wait until a problem happens before you get serious about your security posture.
- Engage a reputable independent third-party to assess your current environment.

AMERICAN STRUCTUREPOINT INC.

IT SOLUTIONS

THANK YOU

Edward “Ed” Valasek

317-508-7321

evalasek@structurepoint.com

https://www.structurepoint.com/it-solutions

Follow Me on LinkedIn: **www.linkedin.com/in/edvalasek**