DGC

ACCOUNTING • TAX • ADVISORY

# American Council of Engineering Companies IT Forum

Nick DeLena, Principal, IT Risk Assurance & Advisory
Scott Goodwin, Manager, IT Risk Assurance & Advisory

October 14, 2021

# DGC FIRM OVERVIEW

**At DGC, our professional curiosity drives everything we do — how we work; how we advise; how we partner with and seek out value for our clients.**

- Regional accounting firm with over 200 employees including 23 Partners, many with Big 4 experience
- Offices in Boston and Woburn
- Significant Partner and Principal involvement in engagements
- Clients include privately-held businesses, their owners, and high net worth individuals
- Tax, Assurance, IT Risk and Business Advisory including valuation, forensic accounting, litigation support, arbitration, transaction advisory services, IT audit, and cybersecurity services.
- Access to global network through membership in Moore Global Network Limited

## WELCOME

# Nick DeLena

**Principal**
IT Risk Assurance
and Advisory

155 Federal Street
Suite 200
Boston, MA 02210
(781) 937 - 5191
ndelena@dgccpa.com

Nick is a Principal in the Business Advisory Group and leads the IT Risk Assurance & Advisory practice. He has more than 20 years of experience providing IT compliance and cybersecurity expertise to clients. Nick's experience includes over 10 years leading IT audit and advisory teams. He has worked with organizations across a variety of industries to assess and improve internal controls, cybersecurity, and IT compliance efforts. Additionally, Nick has over seven years of experience as an IT Operations Manager for an international publicly-traded midcap company.

Nick also holds several leading certifications including the Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), Certified Data Privacy Solutions Engineer (CDPSE), Security+, and the AICPA's SOC for Service Organizations Advanced Practitioner, among others.

**Education**
Brown University, Executive Masters in Business Administration
Suffolk University, Sawyer School of Management, Bachelor of Science in Business Administration in Computer Information Systems, Minor in Finance

# WELCOME

## Scott Goodwin

**Manager**
IT Risk Assurance
and Advisory

155 Federal Street
Suite 200
Boston, MA 02210
(781) 937 - 5722
sgoodwin@dgccpa.com

Scott is a Manager in the firm's Business Advisory Group and a team member of the IT Risk Assurance & Advisory practice. He has extensive experience across a wide variety of areas including vulnerability assessments, infrastructure and application penetration testing, social engineering, along with compliance-focused capabilities including CMMC and DFARS assessment, information security program development and implementation, and fractional CISO services.

Scott holds several industry standard information security and penetration testing certifications including: Certified Ethical Hacker (C|EH), Offensive Security Certified Professional (OSCP), Offensive Security Wireless Professional (OSWP), Security+, Microsoft Security Technology Associate, as well as a number of vendor and technology specific certifications. His experience in the technical areas of the infosec industry has allowed him to identify several previously unknown security vulnerabilities in commercial software during client penetration tests.

### Vulnerability Credits

CVE-2018-11628, CVE-2019-7004, CVE-2019-19774, CVE-2020-12679, CVE-2020-13998, CVE-2020-5132, CVE-2021-27032, CVE-2021-38157

### Education

University of Massachusetts Boston, Bachelors of Science in Physics, Magna Cum Laude

# AGENDA

**Part 1**

- Cybersecurity State of the Union
- Our Perspective on Trends for Engineering Firms
- Recommendations

**Part 2**

- Anatomy of a Penetration Test
- Common External Tactics & Defenses
- Common Internal Tactics & Defenses

# CYBERSECURITY STATE OF THE UNION

**In short, it's not good.**

- Cybersecurity attacks are up **600%** since the start of the COVID-19 Pandemic.
- Some companies are still working remotely or have shifted to a permanent hybrid model.
- Many companies did not have time to upgrade their IT infrastructure before March 2020.
- Ransomware is the most popular malware threat. It has plagued companies across industries and is getting worse. An estimated **31%** of businesses in the United States were affected by ransomware attacks in the last 12 months.

# CYBERSECURITY STATE OF THE UNION

**In short, it's not good.**

- A cyberattack is happening every **14 seconds**.
- One out of three businesses will experience a data breach in the next 2 years.
- **60%** of Small & Medium Business (SMBs) go out of business within six months of a data breach.
- The impact of a data breach is disproportionately larger for smaller organizations between 500 and 1,000 employees at an average cost of **$2.65 million**, or **$3,533** per employee.
- **70%** of SMBs lack the means and capabilities to detect and respond to cyber attacks.

# CYBERSECURITY STATE OF THE UNION

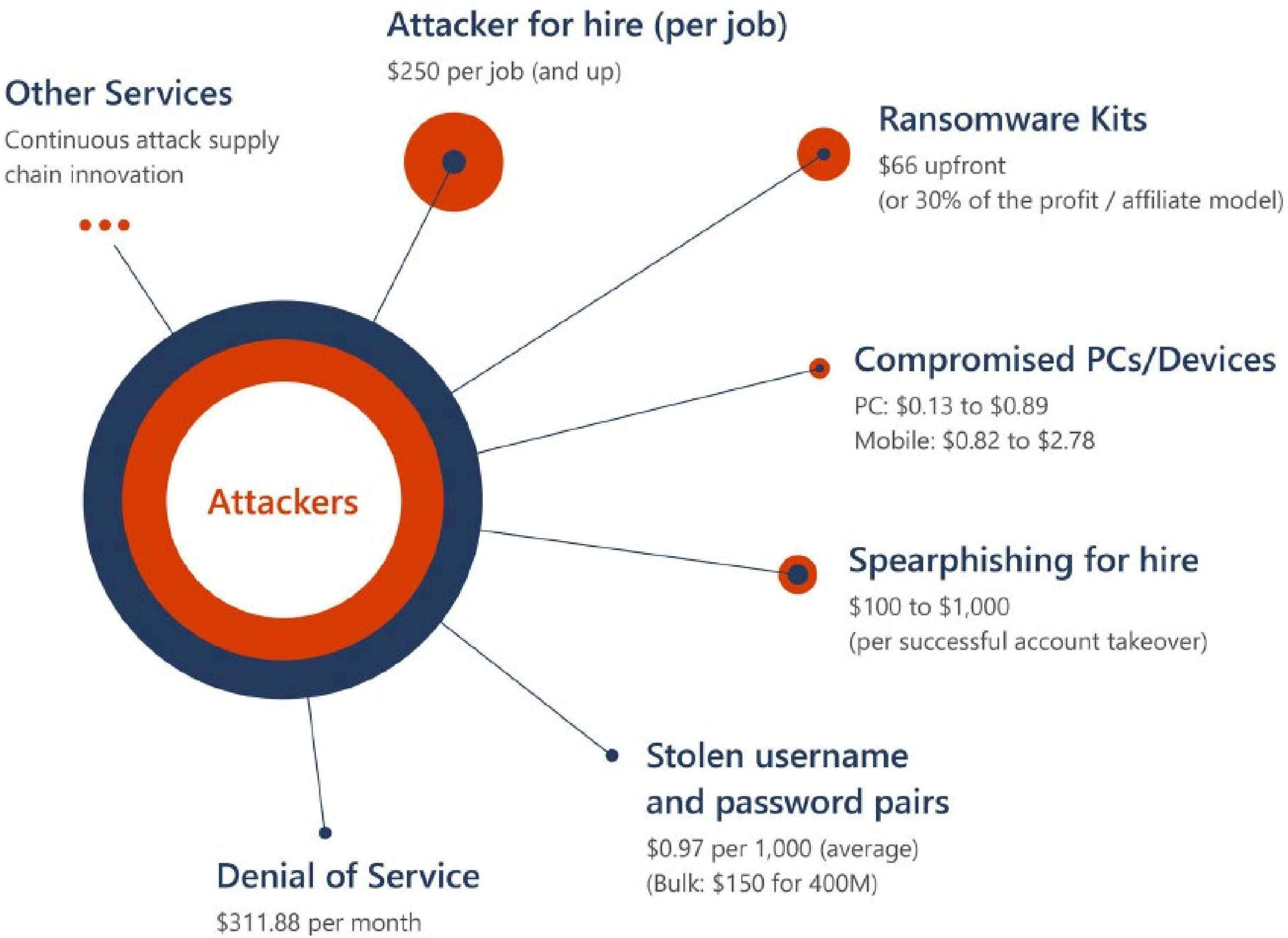
**In short, it’s not good.**

- Cyber criminals are maturing – and so are their business practices.
- Ransomware as a Service is a thing.
- Initial Access Brokers (IABs) are a specific type of malicious actor that is solely focused on obtaining a toehold within vulnerable organizations, then selling that access to ransomware groups.

# CYBERSECURITY STATE OF THE UNION

**In short, it’s not good.**

Average prices of cybercrime services for sale



Attackers

Attacker for hire (per job)
$250 per job (and up)

Other Services
Continuous attack supply chain innovation

Ransomware Kits
$66 upfront
(or 30% of the profit / affiliate model)

Compromised PCs/Devices
PC: $0.13 to $0.89
Mobile: $0.82 to $2.78

Spearphishing for hire
$100 to $1,000
(per successful account takeover)

Stolen username and password pairs
$0.97 per 1,000 (average)
(Bulk: $150 for 400M)

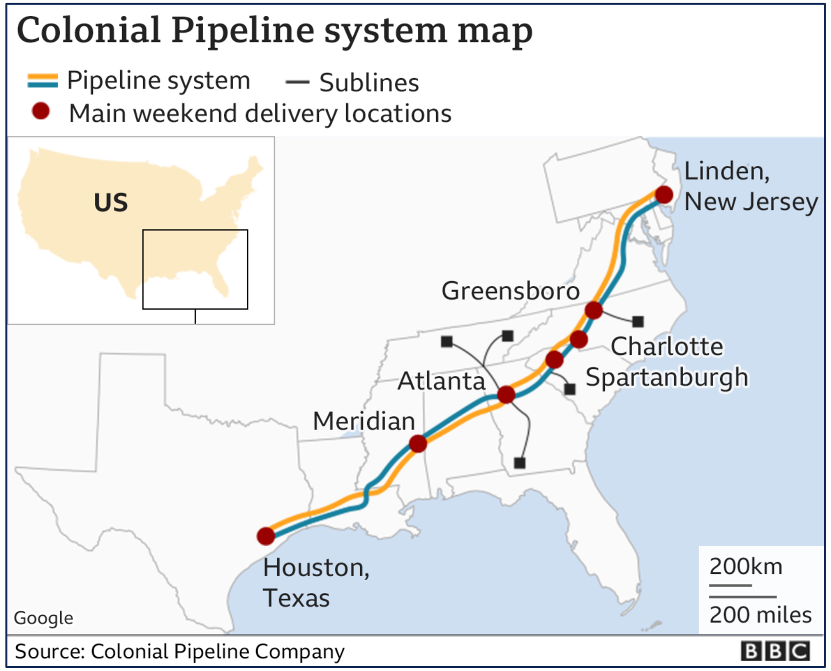
Denial of Service
$311.88 per month

# RECENT BREACHES

| Organization Name | Time Period/Date of Breach | Type of Breach | Industry | Cost of Breach |
|---|---|---|---|---|
| Canon | November 25, 2020 | Ransomware and breach of 10TB of data that include SSN, driver's license numbers, and government-issued identification | Manufacturing | Ransom demand of $4.5 million |
| Kroger | February 20, 2021 | Third party data breach at cloud solutions company, Accellion | Retail | Recovery cost of $5 million in settlement alone |
| Kia Motors | February 18, 2021 | Ransomware attack and breach of corporate data | Manufacturing | Ransom demand of $20 million |
| GEICO | April 19, 2021 | Compromised credentials resulting in stolen license numbers | Insurance | Undisclosed |
| Bose | May 25, 2021 | Ransomware attack and breach of names and SSN | Manufacturing | Ransom demand of $4.4 |
| Guess | July 12, 2021 | Ransomware attack and breach of SSN, driver's license numbers, passport numbers, and financial account numbers | Retail | Undisclosed |
| Facebook | April 3, 2021 | Unsecured API led to exposure of personal data of 533 million Facebook users | Social Media | $3.7 Billion |
| T-Mobile | February 26, 2021 | SIM swap attacks (SIM hijacking) allowed hackers to steal human resource data and pharmacy records | Telecommunications | Undisclosed |
| MultiCare | March 9, 2021 | Ransomware attack and breach of personal information of 200,000 patients | Healthcare | Undisclosed ransom demand |
| CaptureRX | May 7, 2021 | Ransomware attack and breach of names, birthdates, and prescription details of 2 million patients | Healthcare | Ransom demand of $25 million |

# COLONIAL PIPELINE

- Providing 45% of East Coast fuel: gasoline, diesel, heating oil, and jet fuel
- Hacking group known as “DarkSide” targeted the business
- Held information technology systems for ransom
- Stole a significant amount of data to pressure the organization to pay the ransom.
- Proactively halted all operations to mitigate the risk associated with the spread of the malware to OT.
- Colonial paid nearly $5 million for the decryption key



Source: Colonial Pipeline Company

$3.1 billion in assets

$1.3 billion annual revenue

Significant investments in cyber

# KASEYA

- Provider of network and system management software
- Used by outsourced managed service providers to run IT for their own clients
- Compromising the supplier of the software led to compromise of Kaseya clients, as well as clients of MSP’s using the software
- Once the Kaseya tool was compromised, this access was used to deploy ransomware to managed systems.
- 800-1500 individual organizations affected by this single campaign. Over 1 million individual computers.
- Demanded $45,000 – $5 million from each affected organization, or $70 million to restore all affected systems across all organizations.

Information security breaches can directly affect an organization’s clients and partners

# OUR OBSERVATIONS

- IT often does not have representation at the executive level
- Small and medium firms are underinvesting in cybersecurity from a people, process, and technology perspective
- Very few firms have dedicated cybersecurity staff
- Many firms assume their outsourced IT provider is taking a proactive role on cybersecurity matters when oftentimes they are just providing basic IT support
- Many outsourced IT relationships report to non-technical company employees

# OUR OBSERVATIONS

- Relative to other industries, engineering firms are not meeting best practices for similarly-sized companies
- Small and medium firms are not prepared for cyber attacks
  - Lack of tools to detect attack, lack of capabilities to contain and eliminate threats, lack of capacity to respond/recover/report

# OUR OBSERVATIONS

- MAJOR compliance obligations are speeding toward you
  - DOJ recently created the Civil Cyber-Fraud Unit to penalize companies under the False Claims Act (FCA) which hold federal contracts that do not adhere to contractual cybersecurity requirements
  - Applies to ANY contracts with the federal government, including (and especially) the department of defense
  - Contractual flowdowns impact nearly all subcontracting tiers

# THE REGULATIONS

- FAR 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems
- DFARS 252.204-7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting
- ***NEW***: DFARS 252.204-7019 – Notice of NIST SP 800-171 DoD Assessment Requirements
- ***NEW***: DFARS 252.204-7020 – NIST SP 800-171 DoD Assessment Requirements
- ***NEW***: DFARS 252.204-7021 – Cybersecurity Maturity Model Certification (CMMC) Requirements

# THE REGULATIONS – FAR

- FAR 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems
    - Mandates the implementation of 15 technical requirements to protect FCI on the covered contractor information system (anywhere on your infrastructure where information associated with the contract is stored or processed)

# THE REGULATIONS – DFARS 7012

- DFARS 252.204-7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting
  - Triggered when Controlled Unclassified Information (CUI) is expected to be delivered in performance of contract or PO
  - Requires the implementation of the 110 security requirements in NIST Special Publication 800-171
  - By invoicing against a contract with this clause, you indicate you are fully compliant. Compliance has been a self-attestation
  - This is changing through DFARS 252.204-7019 and 7020

# THE REGULATIONS – DFARS 7019/20

- ***NEW***: DFARS 252.204-7019 – Notice of NIST SP 800-171 DoD Assessment Requirements
- ***NEW***: DFARS 252.204-7020 – NIST SP 800-171 DoD Assessment Requirements
  - Defines “basic,” “medium,” and “high” assessment types
  - You must have a current assessment (i.e. not more than three years old) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order, posted in the Supplier Performance Risk System (SPRS) to be considered for award of future work
  - Effective November 30, 2020
  - Applies to primes and subs subject to DFARS 252.204-7012

DGC

# THE REGULATIONS – DFARS 7019/20

- DFARS 252.204-7020 – NIST SP 800-171 DoD Assessment Requirements
  - You must have at a minimum a “basic” self-assessment on file with SPRS
  - The self-assessment must be done using the DoD Assessment Methodology and weighted scoring system
  - These assessments must be filed by CAGE code in SPRS
  - Some organizations will be subject to DoD DCMA DIBCAC-led medium or high assessments

# THE REGULATIONS – CMMC

- ***NEW***: DFARS 252.204-7021 – Cybersecurity Maturity Model Certification (CMMC) Requirements
  - Introduces a third-party certification requirement to verify compliance with FAR and DFARS cyber obligations
  - Offerors with 7021 in an RFI, RFP, or other solicitation, must have the corresponding CMMC certification on file with the DoD prior to taking award
  - Only Certified 3rd Party Assessment Organizations (C3PAOs) can certify
  - To eventually replace DFARS 7019/20
  - Phasing in on a contract-by-contract basis through 2025

# RESOURCES

- NIST 800-171 Security Requirements: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- CMMC Website at DoD: https://www.acq.osd.mil/cmmc/
- CMMC Accreditation Body: https://www.cmmcab.org/
- DFARS Interim Rule Introducing DFARS 7019, 7020, 7021: https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of
- SPRS: https://www.sprs.csd.disa.mil/

# RECOMMENDATIONS

- **Multifactor authentication** – cannot recommend this enough
- Start a cybersecurity working group that develops metrics to measure & report on to management
- Establish a baseline – measure where you stand today against best practices
- Periodically measure your security going forward. Are you getting better? Worse? Have new risks emerged?
- Assess your “cyber resilience” – how well can you withstand and recover from a cyber attack? Have you ever tested your capabilities?
- Look into Zero Trust – an “assume breach” architecture

# QUESTIONS?