SC CYBERSECURITY SUMMIT

WELCOME

Sponsored by:

dew

South Carolina Department of Commerce
Just right for business.

SC MEP
SOUTH CAROLINA MANUFACTURING EXTENSION PARTNERSHIP

Ashely Teasdel
Director | Business Services Division
South Carolina Department of Commerce

Harry M. Lightsey III
Secretary of Commerce
South Carolina Department of Commerce

Dr. Cynthia Davis
Business & Industry Programs Manager
SC Department of Commerce

Lieutenant Sean Fay
SC Cyber Coordination Center (SC C^3)
SC Critical Infrastructure Cybersecurity (SC CIC) Program
South Carolina Law Enforcement Division


48%
System HACKED

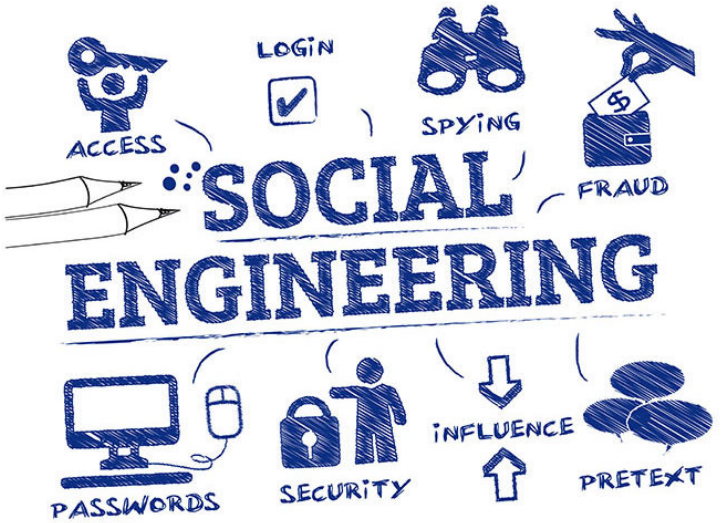
South Carolina

Critical Infrastructure Cybersecurity Program

What is Social Engineering?

so·cial en·gi·neer·ing
/ˈsōSHəl ˌenjəˈni(ə)riNG/

noun
the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.



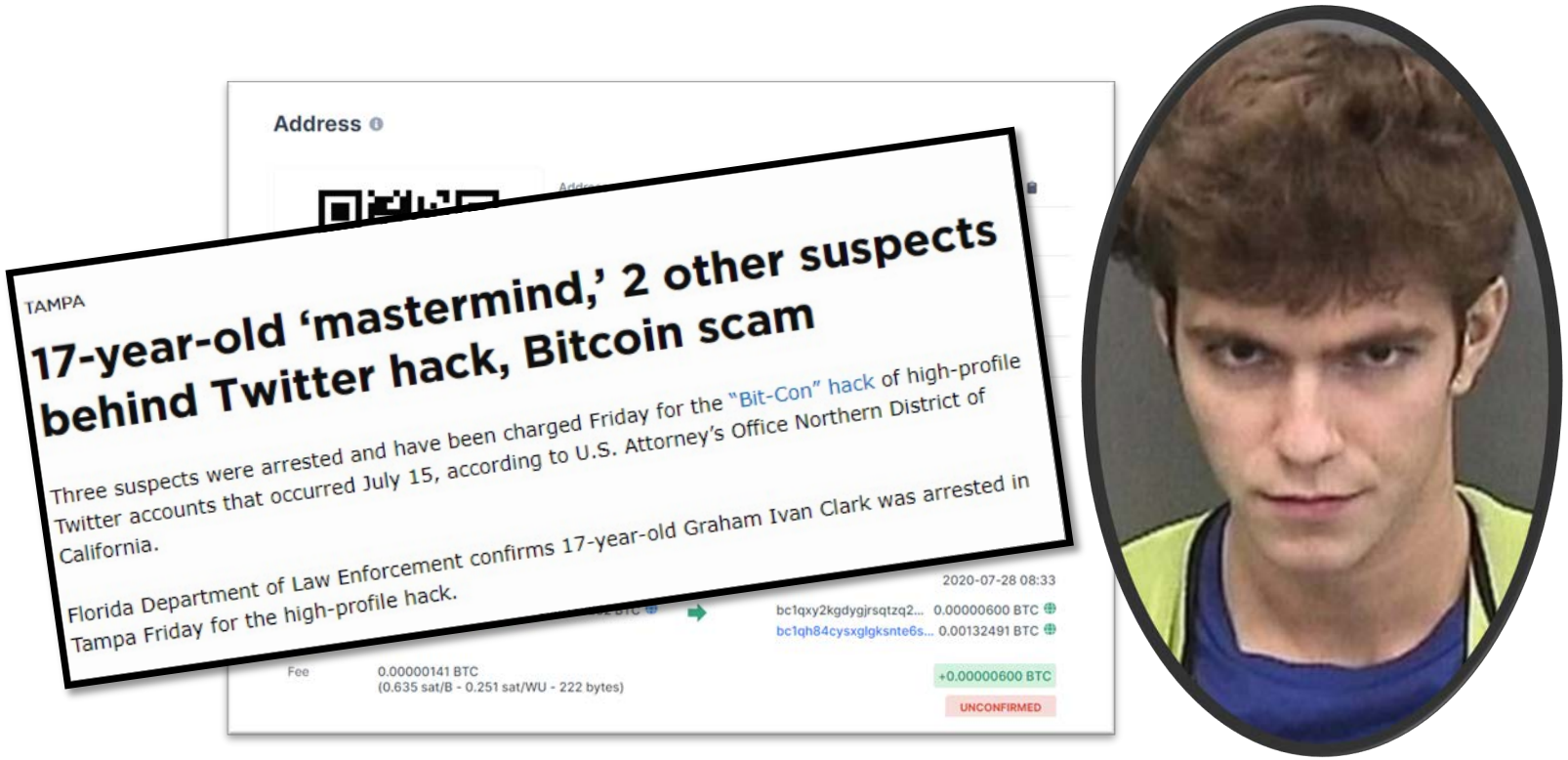
Social Engineering on Twitter

July 2019 - Twitter: The attackers successfully manipulated a small number of employees and used their credentials to access Twitter's internal systems, including getting through our two-factor protections. As of now, we know that they accessed tools only available to our internal support teams to target 130 Twitter accounts. For 45 of those accounts, the attackers were able to initiate a password reset, login to the account, and send Tweets."

The forty-five included: Bill Gates, Elon Musk, Jeff Bezos, Kanye West, Uber, Apple, Barack Obama, and Joe Biden.

Social Engineering on Twitter

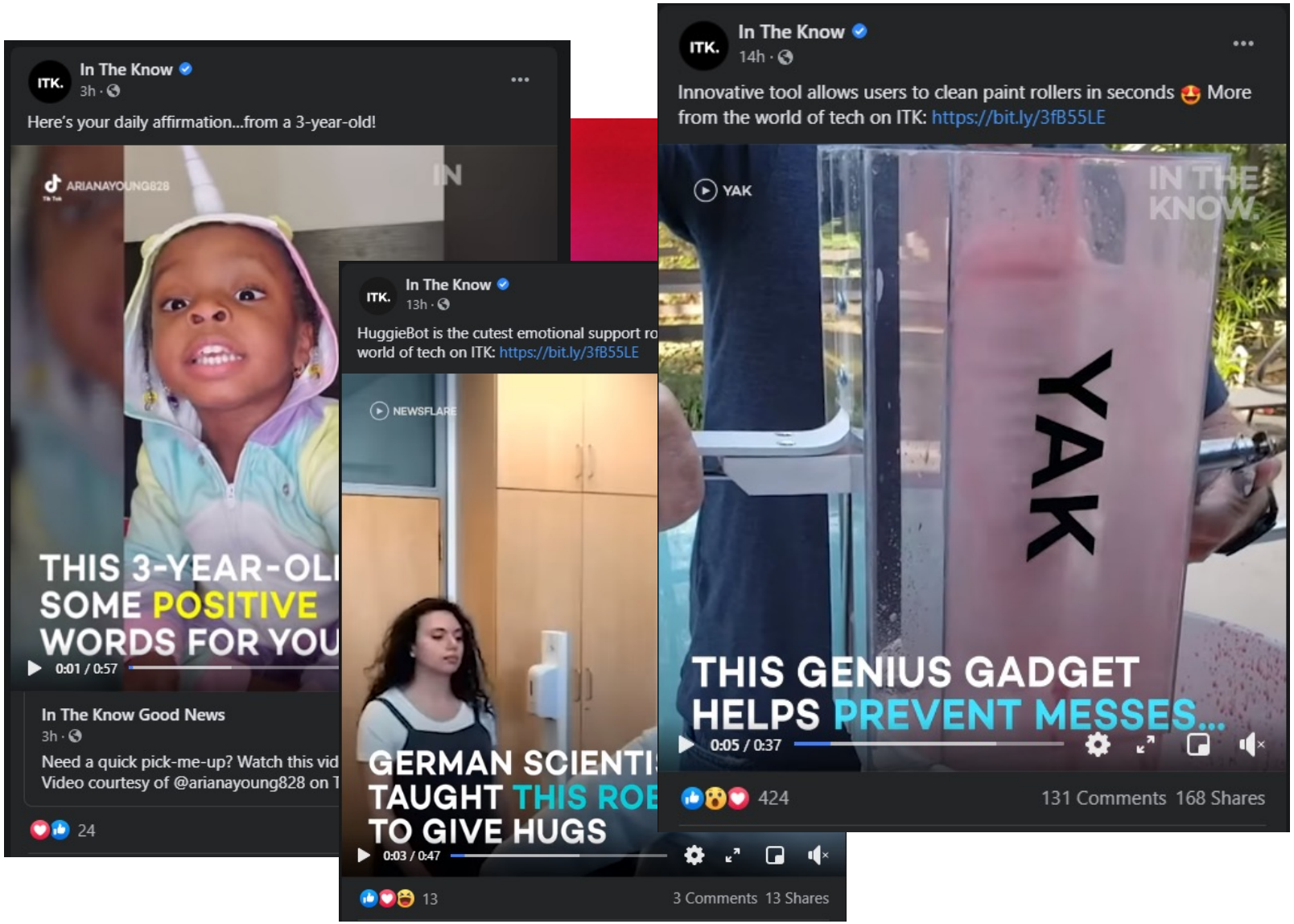
Social Engineering on Twitter



12.87 BTC = **$144,573.86** (as of July 29, 2020)

12.87 BTC = **$636,032.83** (as of February 24, 2021)

Disinformation on Facebook?



Page Transparency

In The Know
News & Media Website

Organizations That Manage This Page

The person or group responsible for this Page hasn't completed our verification process yet.

Page History

Merged with the Page Broternity
June 10, 2020

Merged with the Page In The Know: Life
September 17, 2018

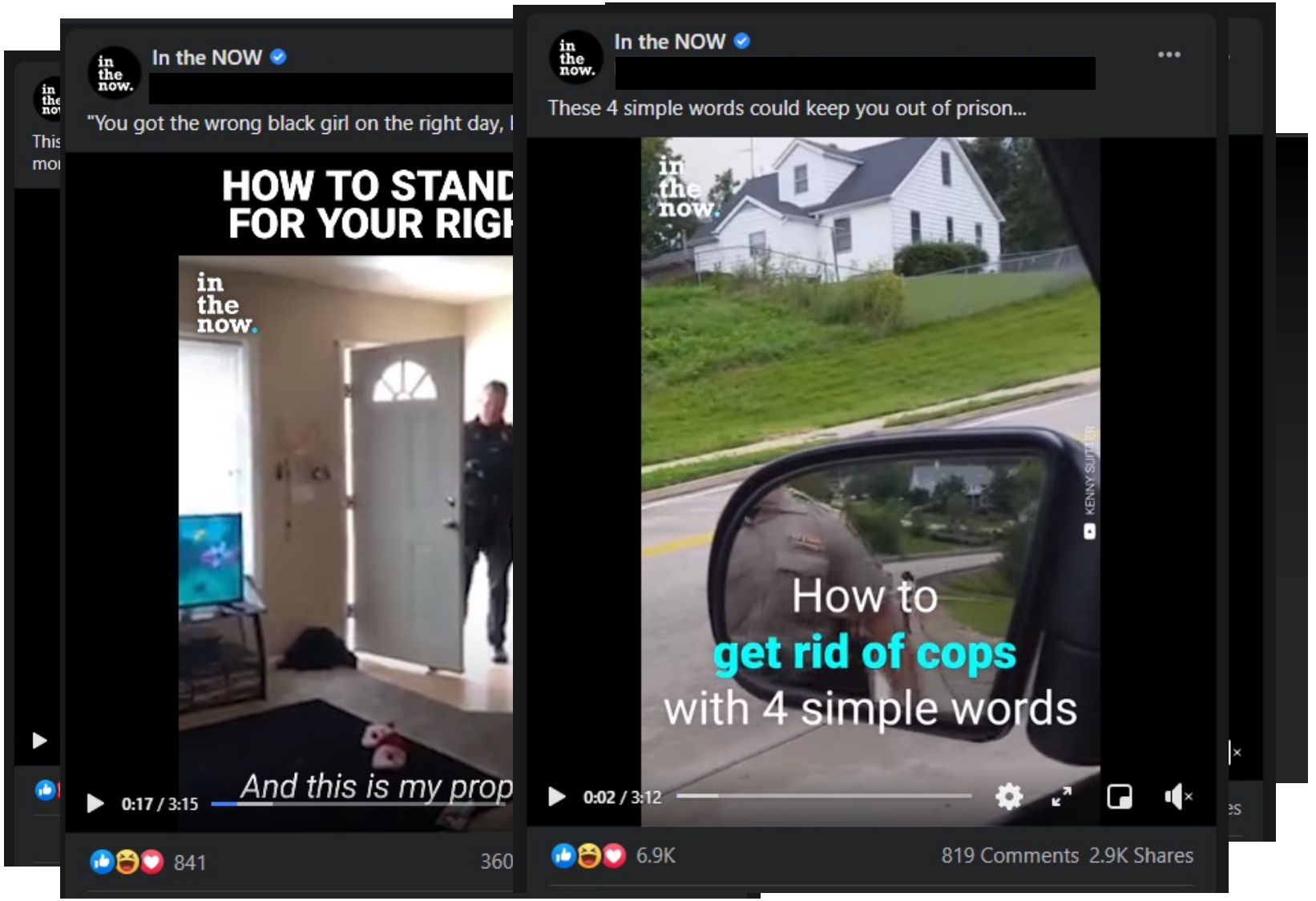
Changed name to In The Know
July 20, 2016

See 2 More

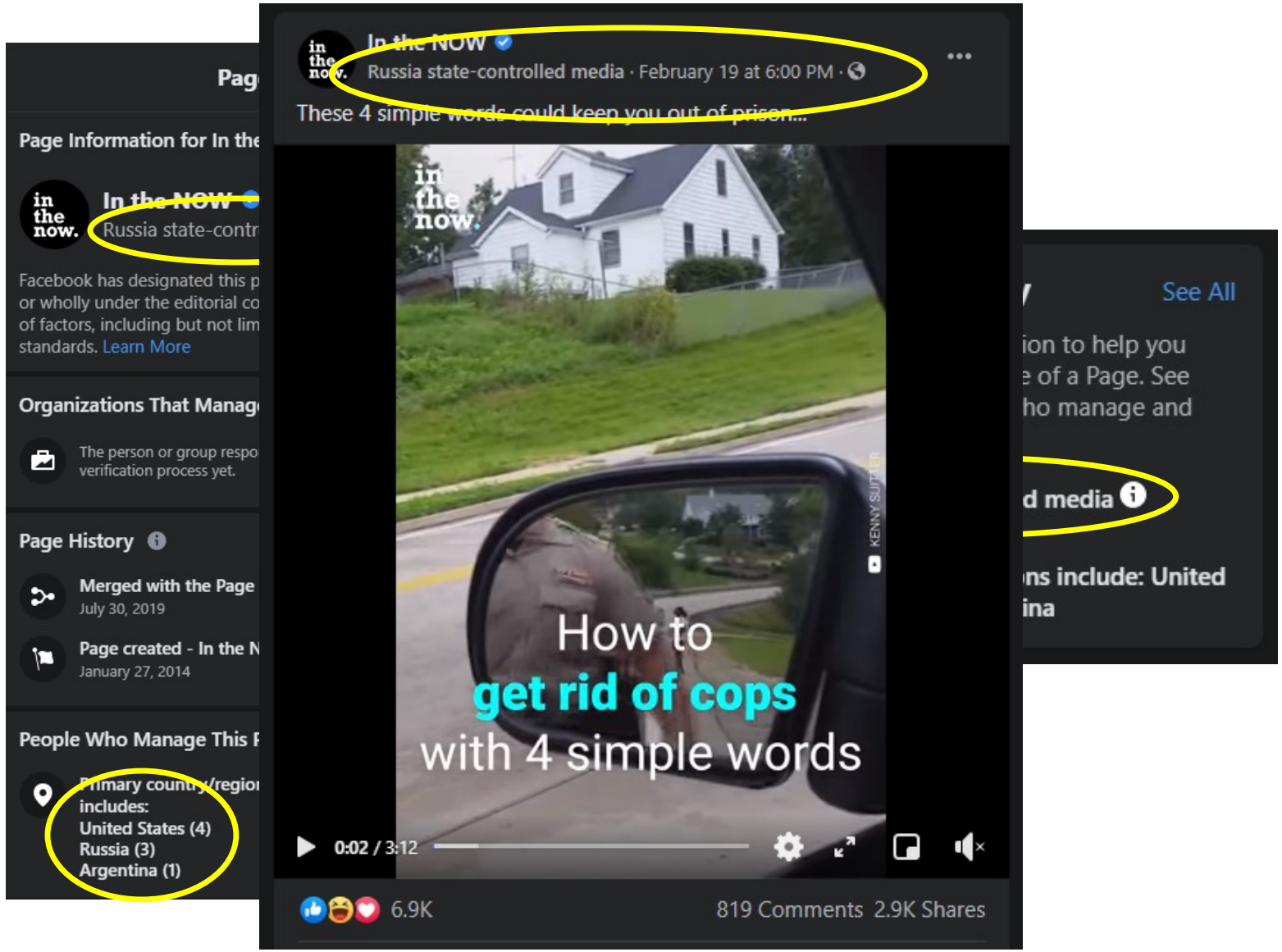
People Who Manage This Page

Primary country/region location for people who manage this Page includes:
United States (93)
Australia (5)
Hong Kong (1)
Singapore (1)
Taiwan (1)

Disinformation on Social Media



Disinformation on Social Media



Disinformation on Social Media

Support the Guardian
Available for everyone, funded by readers
Contribute → Subscribe →

Search jobs | Sign in | Search | US edition

The Guardian
For 200 years

News | Opinion | Sport | Culture | Lifestyle | More

Australia Coronavirus World AU politics Environment Football Indigenous Australia Immigration Media Business Science Tech

Marketing & PR

Influencers say Russia-linked PR agency asked them to disparage Pfizer vaccine

Fazze offered money to YouTubers and bloggers to falsely claim jab was responsible for hundreds of deaths

- Coronavirus - latest updates
- See all our coronavirus coverage

Jon Henley *Europe correspondent*
@jonhenley
Tue 25 May 2021 10.17 EDT

https://www.theguardian.com/media/2021/may/25/influencers-say-russia-linked-pr-agency-asked-them-to-disparage-pfizer-vaccine

Disinformation on Social Media

https://www.nytimes.com/2015/06/07/magazine/the-agency.html

What is Cybersecurity?

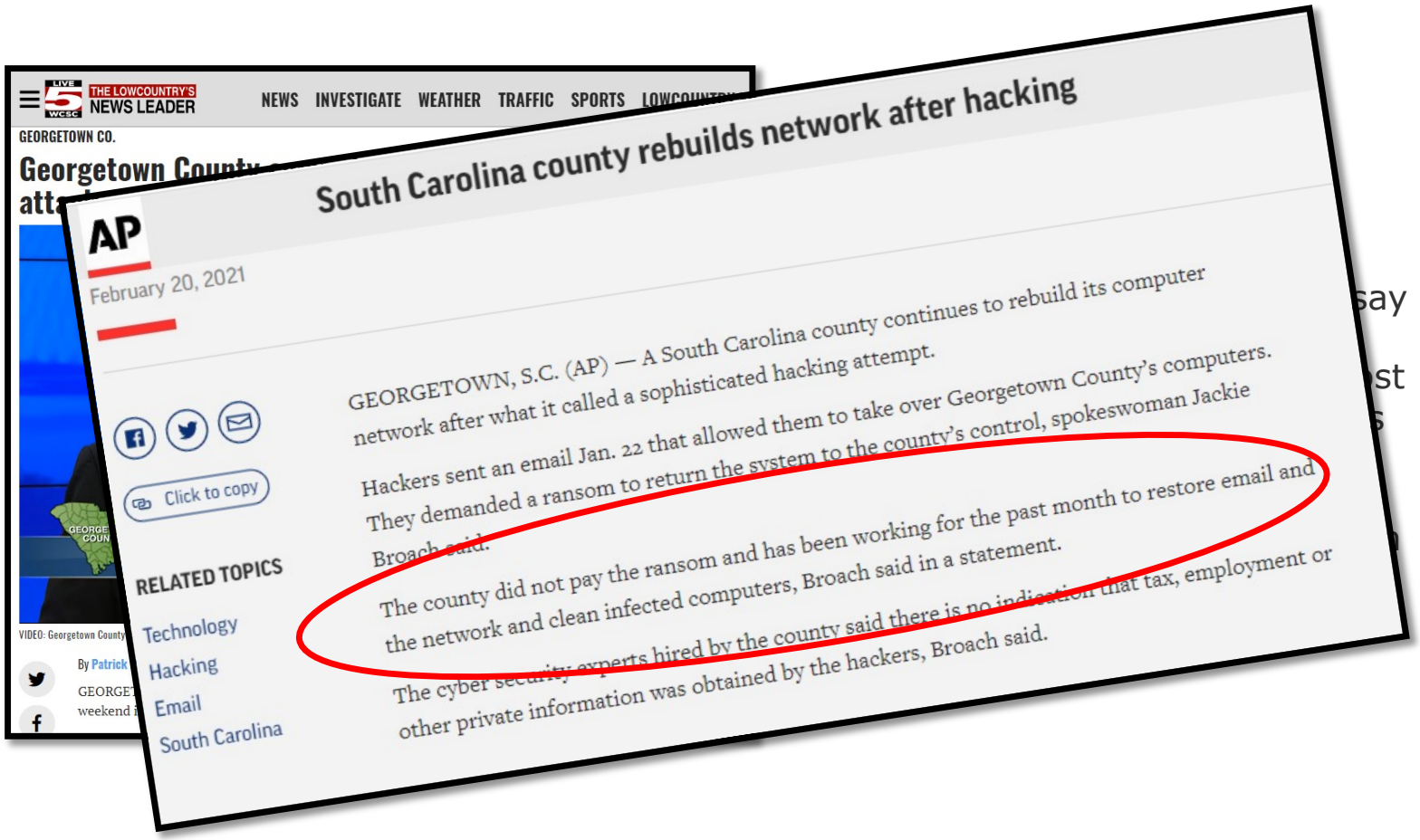
Definition of Cybersecurity

noun: measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

Simply put, cybersecurity is protection against digital attacks.

The Department of Homeland Security says it best: "Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace."

Georgetown County, SC



THE LOWCOUNTRY'S NEWS LEADER

NEWS INVESTIGATE WEATHER TRAFFIC SPORTS

GEORGETOWN CO.

Georgetown County

VIDEO: Georgetown County

By Patrick

GEORGE

weekend

AP

February 20, 2021

South Carolina county rebuilds network after hacking

GEORGETOWN, S.C. (AP) — A South Carolina county continues to rebuild its computer network after what it called a sophisticated hacking attempt.

Hackers sent an email Jan. 22 that allowed them to take over Georgetown County's computers. They demanded a ransom to return the system to the county's control, spokeswoman Jackie Broach said.

The county did not pay the ransom and has been working for the past month to restore email and the network and clean infected computers, Broach said in a statement.

The cyber security experts hired by the county said there is no indication that tax, employment or other private information was obtained by the hackers, Broach said.

Click to copy

RELATED TOPICS

Technology

Hacking

Email

South Carolina

Georgetown County, SC

U.S. DEPARTMENT OF THE TREASURY

ABOUT TREASURY | POLICY ISSUES | DATA | SERVICES | NEWS

NEWS

- Press Releases
  - Statements & Remarks
  - Readouts
  - Testimonies
- Featured Stories
- Press Contacts

PRESS RELEASES

Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware

220

December 5, 2019

Washington – Today the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) took action against Evil Corp, the Russia-based cybercriminal organization responsible for the development and distribution of the Dridex malware. Evil Corp has used the Dridex malware to infect computers and harvest login credentials from hundreds of banks and financial institutions in over 40 countries, causing more than $100 million in theft. This malicious software has caused millions of dollars of damage to U.S. and international financial institutions and their customers. Concurrent with OFAC's action, the Department of Justice charged two of Evil Corp's members with criminal violations, and the Department of State announced a reward for information up to $5 million leading to the capture or conviction of Evil Corp's leader. These U.S. actions were carried out in close coordination with the United Kingdom's National Crime

Georgetown County, SC

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: October 1, 2020

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. This advisory describes these sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.[2]

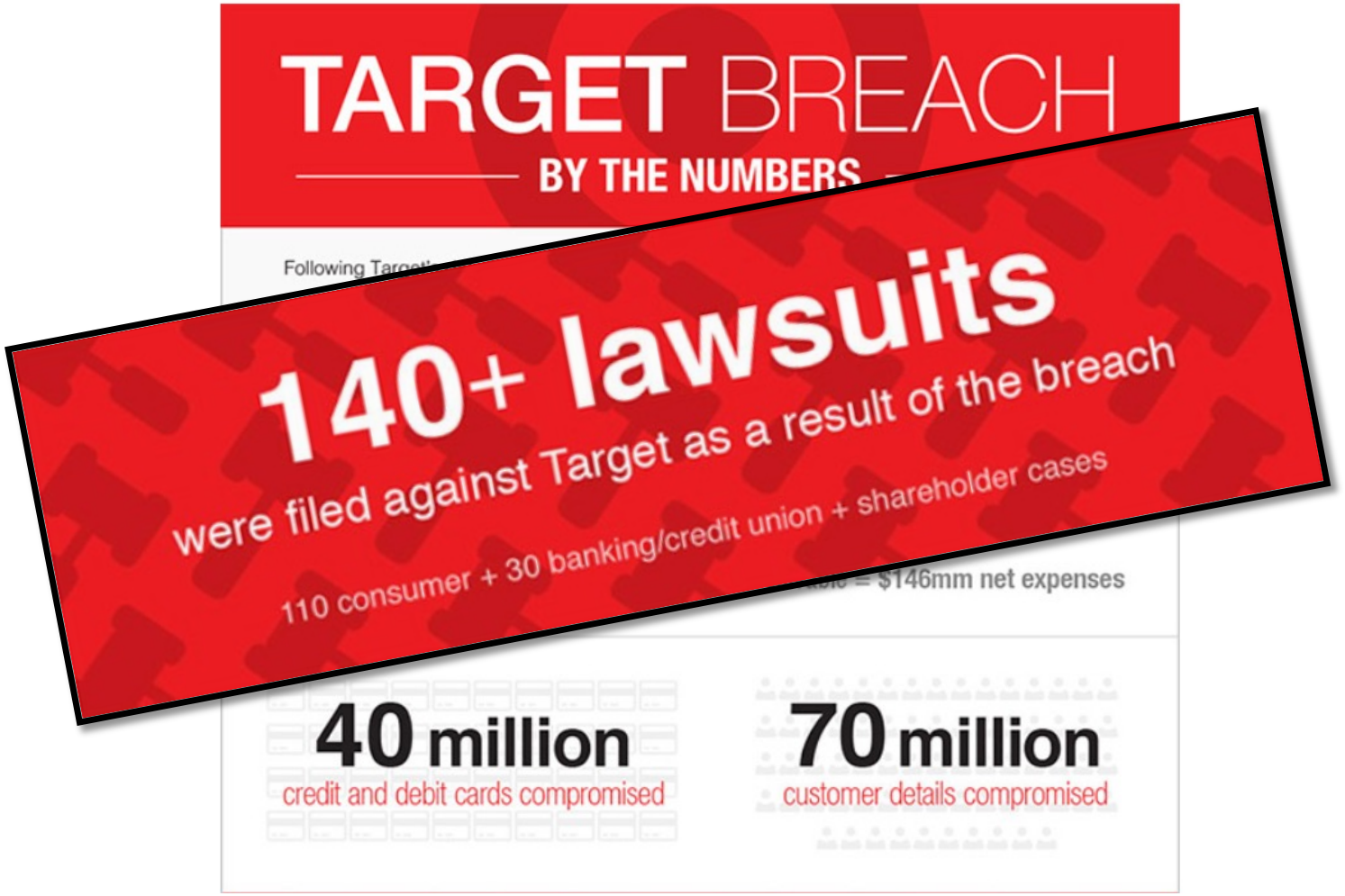
Target incident

A small heating and air conditioning firm in Pennsylvania that worked with Target and had suffered its own breach via malware discovered in an email.

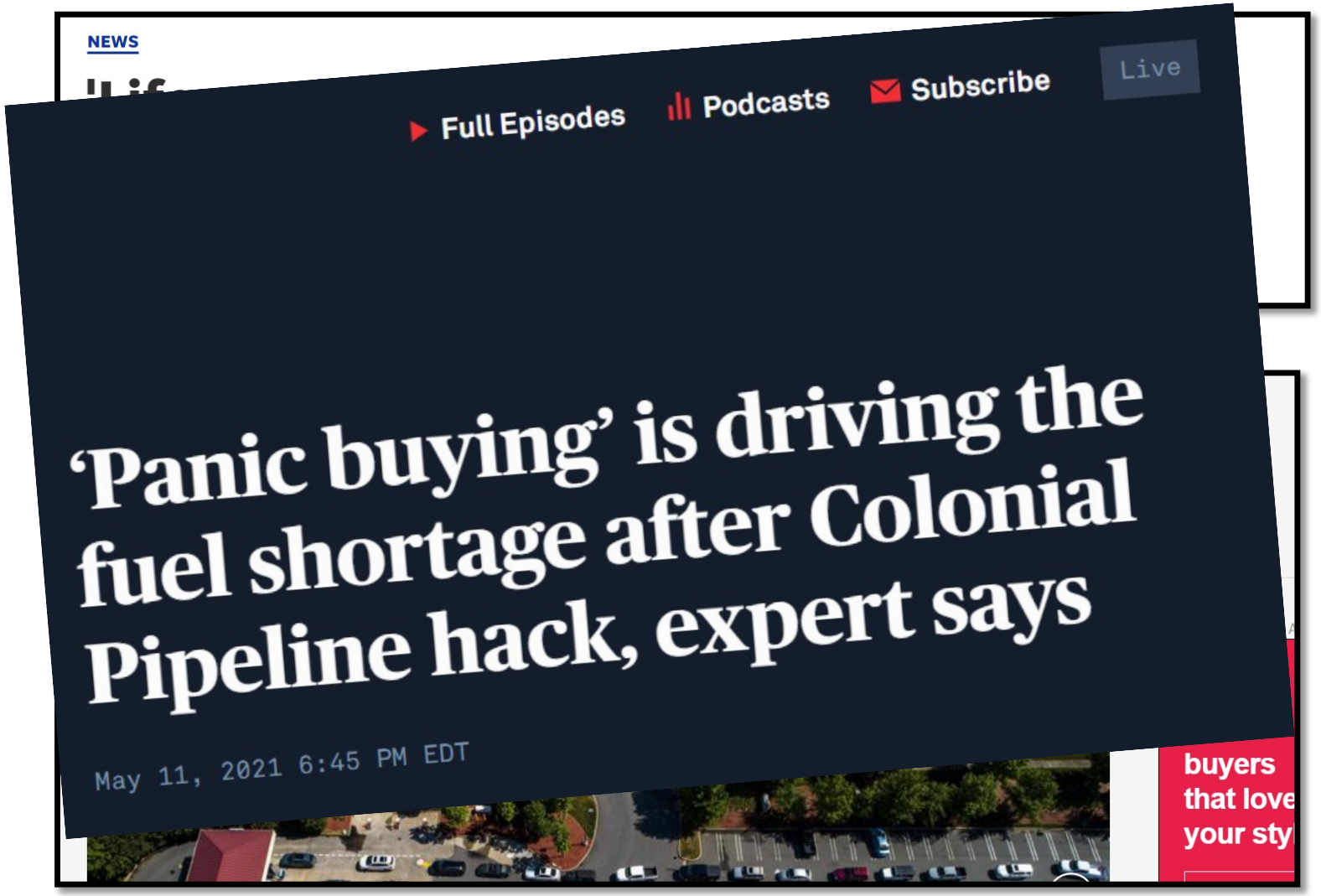
In that intrusion, the thieves managed to steal the virtual private network credentials that the firm's technicians used to remotely connect to Target's network.

Hackers used that initial foothold provided by the firm's hack to push malicious software down to all cash registers at more than 1,800 stores nationwide.

Target incident



Colonial Pipeline incident



Colonial Pipeline incident

May 12, 2021
7:02 PM EDT

Energy

Menu Search **Bloomberg** Sign In

Cybersecurity

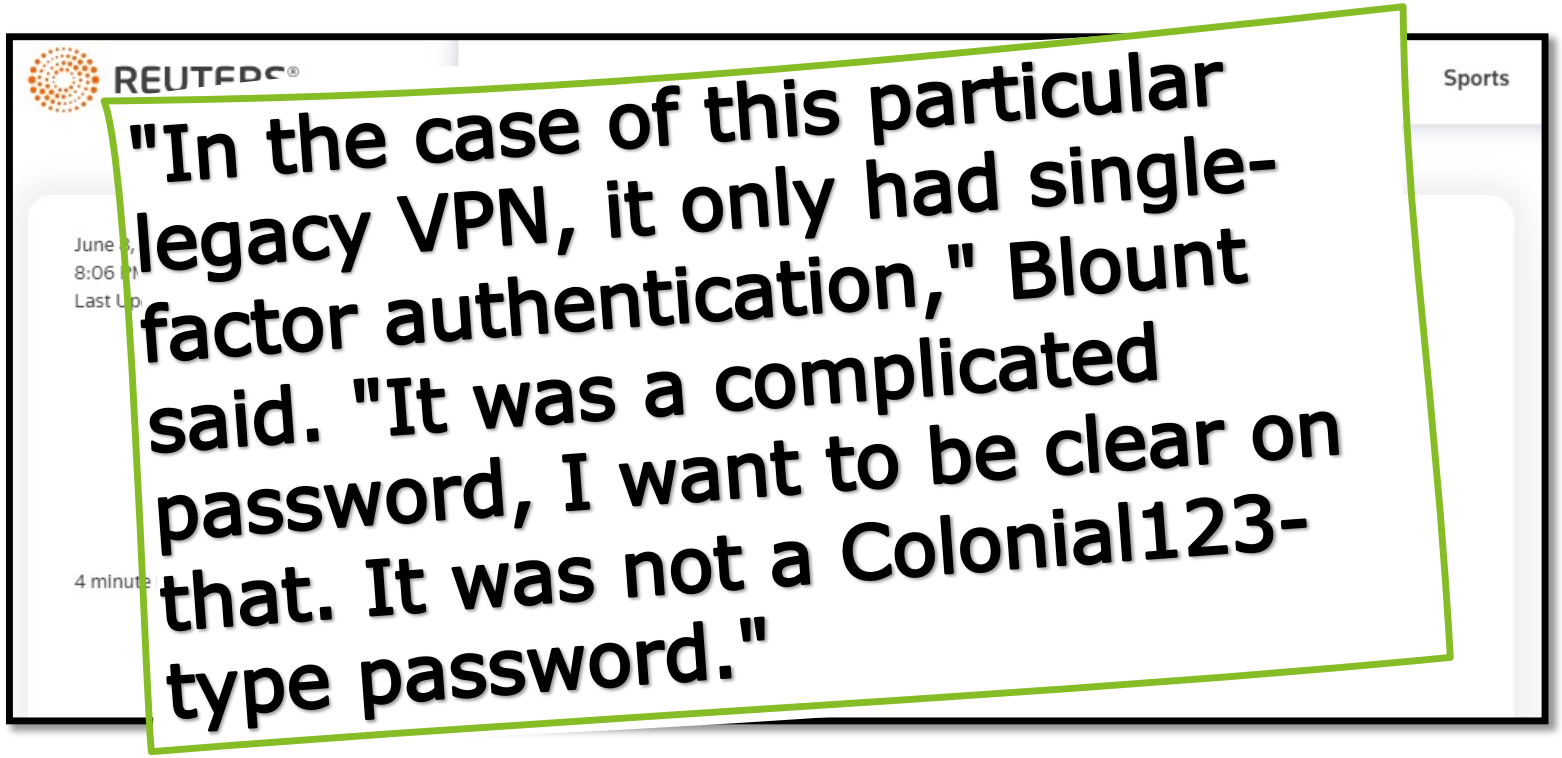
Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom

By William Turton, Michael Riley, and Jennifer Jacobs
May 13, 2021, 10:15 AM EDT *Updated on May 13, 2021, 7:01 PM EDT*

- Payment came shortly after attack got underway last week
- FBI discourages organizations from paying ransom to hackers

It's not

Colonial Pipeline incident



JBS incident

MORNING BRIEF

Foreign Policy's flagship daily newsletter with what's coming up around the world today. Delivered weekdays.

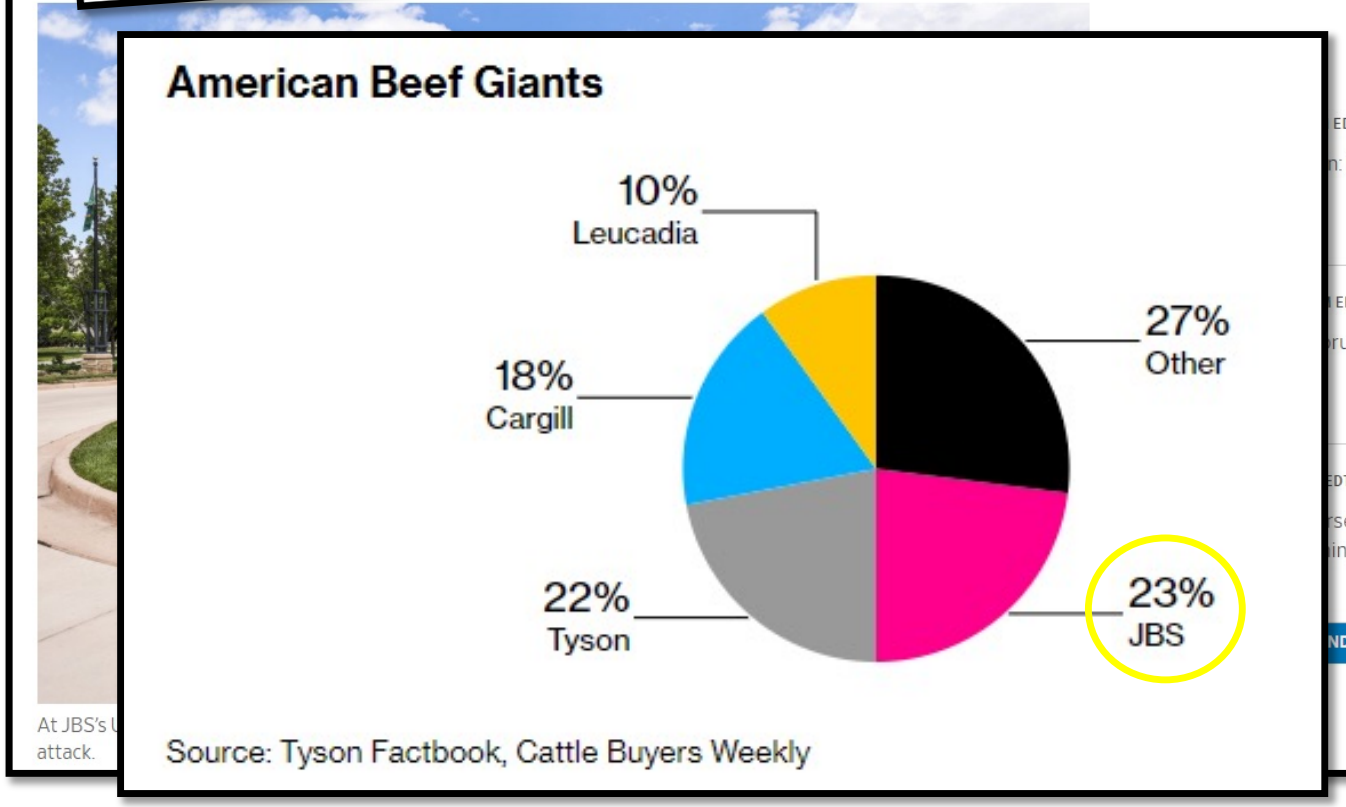
U.S. Meat Industry Becomes Latest Cyber Victim

A ransomware attack forced the world's largest meat producer to close all U.S. beef plants at a time when global meat prices are already soaring.

By Colm Quinn, the newsletter writer at *Foreign Policy*.

JBS incident

A cyberattack on JBS SA, the largest meat producer globally, forced the shutdown of all its U.S. beef plants, wiping out output from facilities that supply almost a quarter of American supplies.



JBS incident

NEWS

Beef supplier JBS paid ransomware hackers $11 million

SHARE THIS –

SECURITY

Beef supplier JBS paid ransomware hackers $11 million

The company was hacked in May by a Russian-speaking hacker gang, which led meat plants across the U.S. and Australia to shut down for at least a day.

New Orleans, LA Incident

Phishing

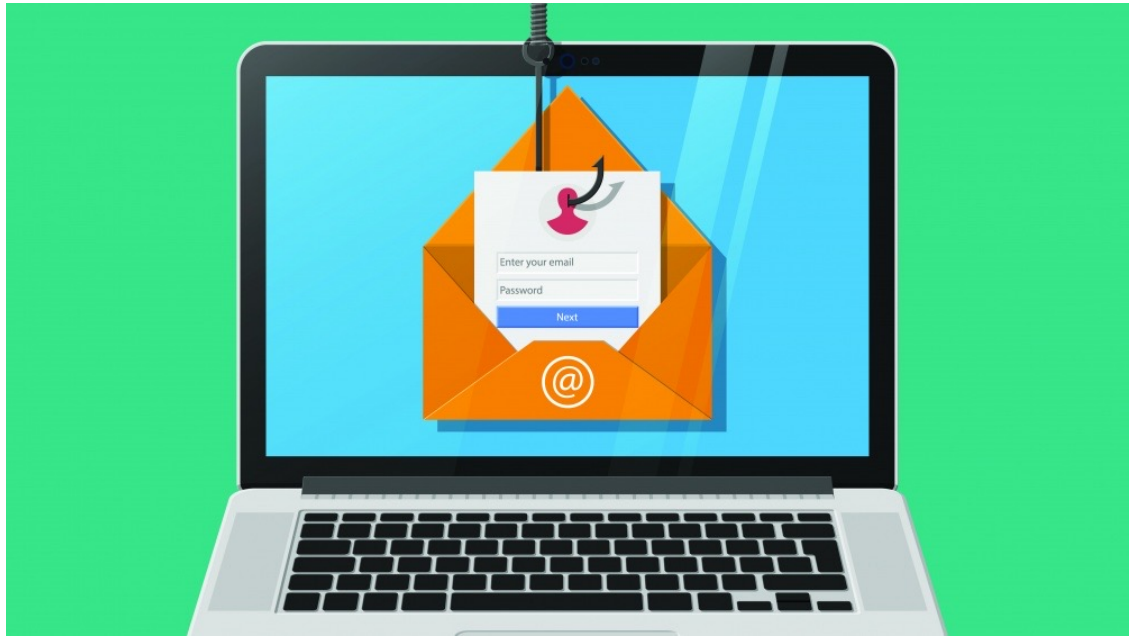
phish·ing
/ˈfiSHiNG/

noun
the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. "an email that is likely a phishing scam"

Phishing

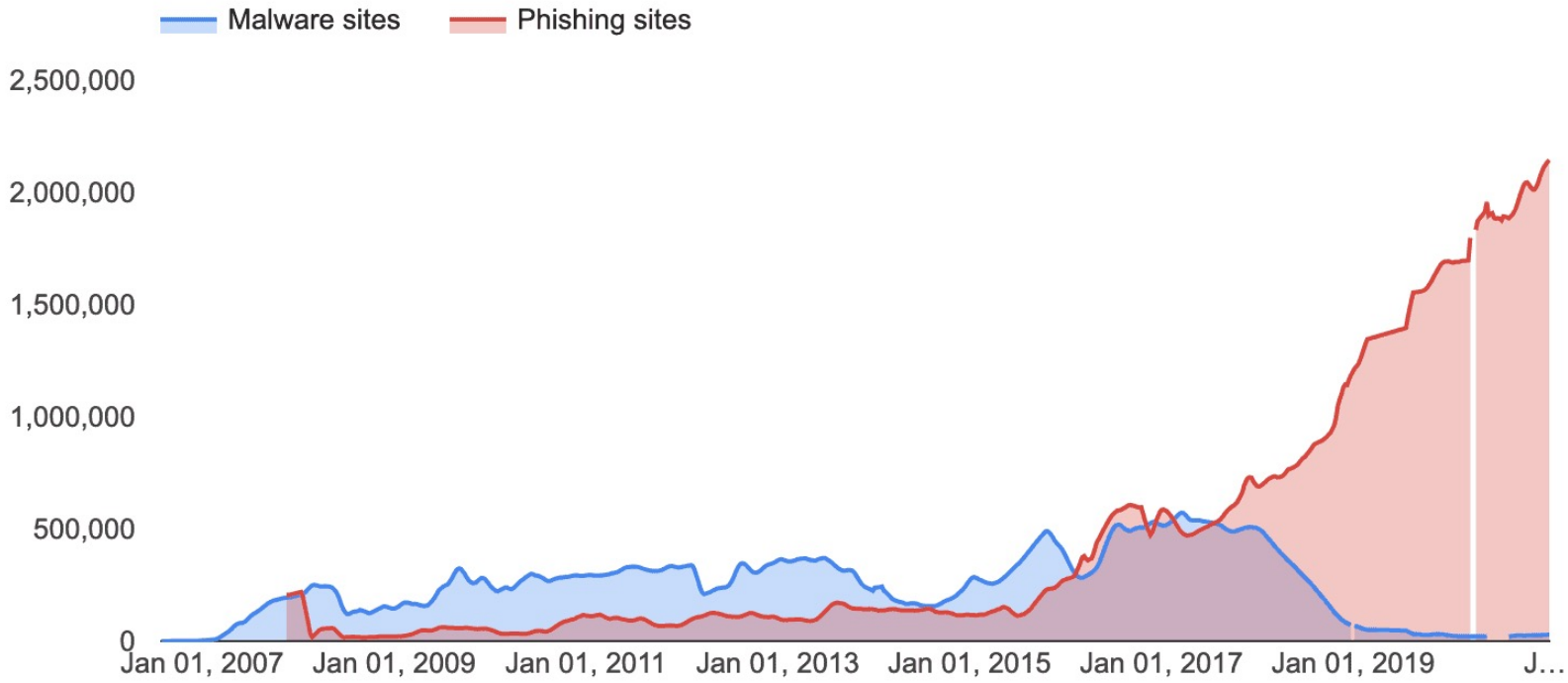
According to Security Intelligence, in 2019, attackers used phishing as an entry point for almost one-third of all cyber attacks.

The COVID-19 pandemic has only made things worse. Phishing attacks have increased by a massive 600% since the end of February 2020, as bad actors seek to exploit the fear and uncertainty of the current moment.



Phishing

From Google Safe Browsing



Google has registered 2,145,013 phishing sites as of Jan 17, 2021?
This is up from 1,690,000 on Jan 19, 2020 (up 27% over 12 months)

Leaked Credentials

- The Verizon 2021 Data Breach Investigations Report found that 61 percent of data breaches are caused by leaked credentials.

  Credentials are highly sought out by hackers!

- The largest password leak in history occurred in June 2021; a collection of 8.4 billion passwords make up the stolen credential forum, further proving the value of stolen credentials, whether personal or professional.

Cyber crime by the numbers

Let's put it in perspective:

- Tesla, Facebook, Microsoft, Apple, Amazon, and Walmart combined annual revenue totals "just" $1.28 trillion. Cyber crime earns $1.5 trillion annually.
- The $1.5 trillion that cybercriminals earn is equal to Russia's gross domestic product (GDP)
- If cybercrime were a country, it would have the 13th highest GDP in the world.

Cyber crime by the numbers

Let's put it in perspective:

- It's estimated that cybercrime will cost the world $10.5 trillion annually by 2025.
- Organized criminal gangs account for 55% of attacks

How can we stop it?

1. Be prepared by having full backups. Then test your backup process.

2. Patch. Patch. Patch.

3. Train ALL employees on phishing and cybersecurity training both IN PERSON and online.

4. Implement multi-factor authentication for ANY external access (email, OneDrive, VPN) and for any domain admin account.

5. Test your CSIRT (Cybersecurity Incident Response Team) and incident response plan! You're not too small or too large!

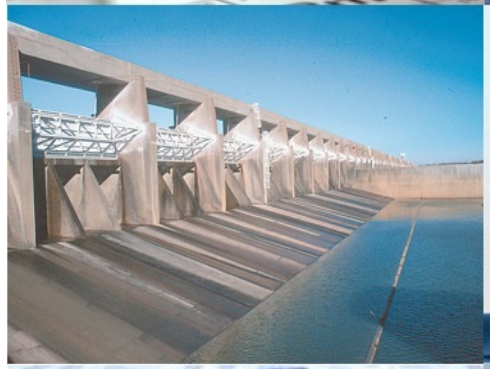
6. Trust but verify. Have a third party come in for an audit. You don't know what you don't know.

7. Join our free program!

South Carolina Critical Infrastructure Cybersecurity Program





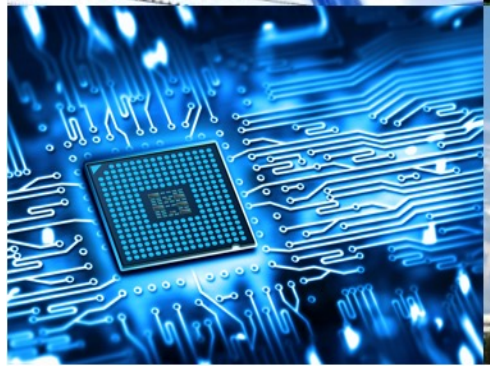


SOUTH
CAROLINA
541



DOW JONES






SC Cyber Coordination Center

EXTERNAL VULNERABILITY SCANNING

CYBER THREAT INFORMATION & INTELLIGENCE

INCIDENT RESPONSE DURING CRITICAL CYBER EVENTS

CYBERSECURITY TRAINING AND RESOURCES

Questions?

To get more information on our free program, email me at clo@sled.sc.gov

SC CYBERSECURITY SUMMIT

IT Cybersecurity Infrastructure Panel

Sponsored by:

dew

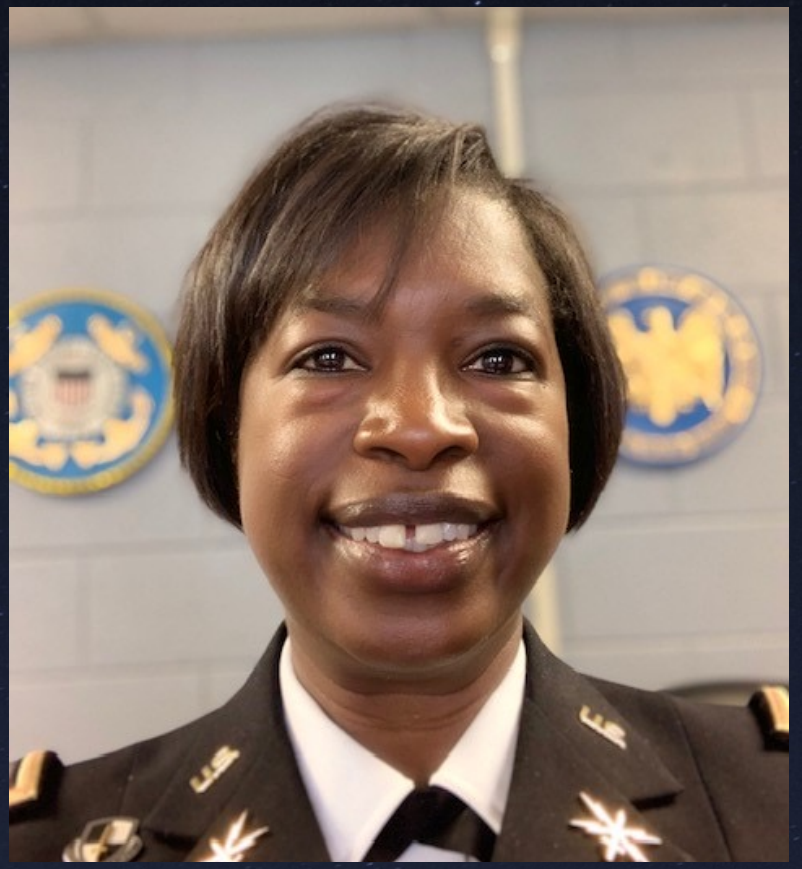
South Carolina Department of Commerce
Just right for business.

SC MEP
SOUTH CAROLINA MANUFACTURING EXTENSION PARTNERSHIP

Sue-Ann ("Susie") Gerald Shannon
President & CEO
South Carolina Council on Competitiveness

Erik J. Gardner
Palmetto Tech Bridge Outreach Coordinator
Naval Information Warfare Center Atlantic

Mark A. Lester MBA, CISSP
Manager Information Security
South Carolina Ports Authority



Linda Riedel, COL SCARNG
Deputy Director of Operations and Outreach
Citadel DoD Cyber Institute (CDCI)
Cyber and Computer Science Department

SC CYBERSECURITY SUMMIT

Cybersecurity Maturity Model Certification CMMC

Sponsored by:

dew

South Carolina Department of Commerce
Just right for business.

SC MEP
SOUTH CAROLINA MANUFACTURING EXTENSION PARTNERSHIP

Roy Luebke
Innovation and Growth Consultant
GENEDGE

GENEDGE

CMMC:
Cybersecurity Maturity Model Certification

Roy Luebke | September 1, 2021

PART OF THE MEP National Network™

About GENEDGE

- GENEDGE Alliance (GENEDGE) is a public-private partnership that empowers small and medium-sized Virginia manufacturers to grow and thrive through educational resources, industry connections and best practices through customized solutions to solve their operational and business challenges. GENEDGE delivers to over 200 companies each year in Virginia .

- In 1994, GENEDGE became part of the Manufacturing Extension Partnership (MEP) National Network™ comprised of 51 MEP Centers located in all 50 states and Puerto Rico. The network provides any U.S. manufacturer with access to resources needed to succeed from its more than 1,400 trusted advisors and experts at approximately 375 MEP service locations nationwide.

GENEDGE

Today's Overview

1. **How CMMC came into being – history**

2. **DFARS 7012/CUI brief overview**
   - **System Security plan**
   - **Incident response plan**
   - **Plan of Action/milestones for the gaps vs. NIST 800-171**

3. **CMMC Levels 1-5: Definitions (non-CUI)**

4. **What is a C3PAO and how/what to get audited**

5. **Other important information**
   - **Technical**
   - **Policy and procedure**
   - **Email/file storing**
   - **Multi factor authentication**
   - **Physical security issues**
   - **Staff on-going training**

How CMMC came into being - history

- October 2019 announcement meeting
- DFARS 253.204-7012 is parent regulation
- All rules are created by DoD
- CMMC Accreditation Body trains assessors, authorizes C3PA0s, issues certifications

  www.cmmcab.org

Key Terms:

CUI: Controlled Unclassified Information

•Government created or owned UNCLASSIFIED information that must be safeguarded from unauthorized disclosure.

•An overarching term representing many difference categories, each authorized by one or more law, regulation, or Government-wide policy.

•Information requiring specific security measures indexed under one system across the Federal Government.

- **FOR BOTH PRIMES AND SUBCONTRACTORS**

https://www.dodcui.mil/Home/DoD-CUI-Registry/

https://www.archives.gov/cui/registry/category-list

Key Terms:

FCI: Federal Contract Information

- ***Federal contract information*** means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

- ***Covered contractor information system*** means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

- ***Information*** means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

- ***Information system*** means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information

DFARS 7012 – What you need to have:

1. **System Security plan**
2. **Incident response plan**
3. **Plan of Action/milestones for the gaps vs. NIST 800-171 Specifications**

Only in effect for CUI

GENEDGE

What Regulations Are Driving This?

DFARS 252.204-7012

DFARS 252.204-7019

DFARS 252.204-7020

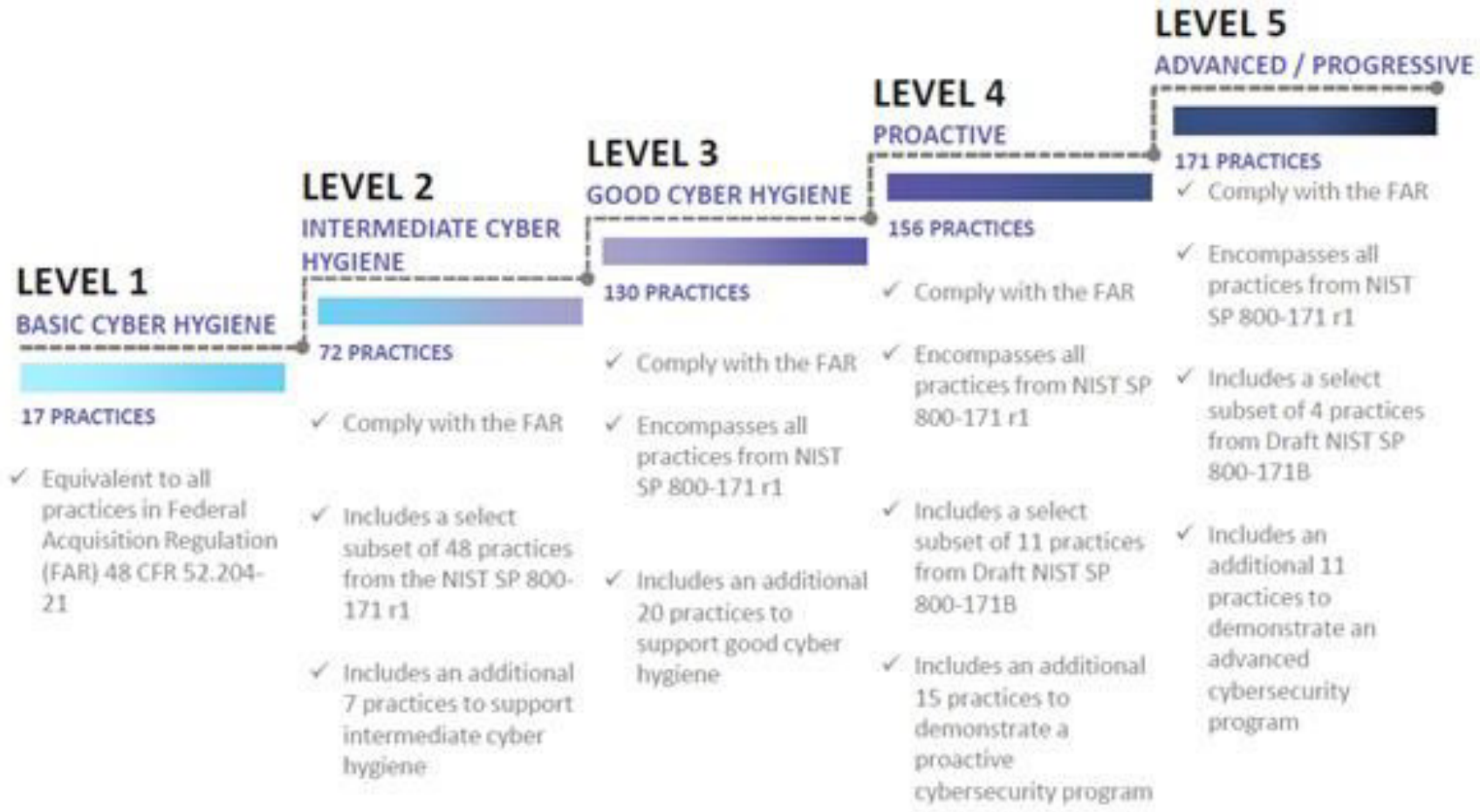
DFARS 252.204.7021

CMMC Levels 1-5: Definitions (non-CUI)

CMMC stands for “Cybersecurity Maturity Model Certification” and is a unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB). The CMMC framework includes a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the Department that a DIB company can adequately protect sensitive unclassified information, accounting for information flow down to subcontractors in a multi-tier supply chain.

www.cmmcab.org

CMMC Levels 1-5: Definitions (non-CUI)

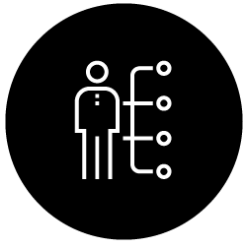


CMMC Organizations

C3PAO

Assessors

Registered Provider Organization



Registered Practitioners

Organizations Seeking Certification

Licensed Partner Publisher

Licensed Training Providers

What is a C3PAO and how/what to get audited

(CMMC Third Party Assessment Organization)

CMMC Marketplace: https://cmmcab.org/marketplace/

C3PAOs hire (or contract) Certified Assessors who YOU hire and PAY to conduct an audit and give your company a CERTIFICATION LEVEL

The key is MATURITY – EVIDENCE OF OPERATIONS

Other Important Information:

SPRS – Supplier Performance Risk System (you must self score with current contract with 7012)

Technical issues

Policy and procedure development

Email/file storing i.e. MS O365 GCC High

Multi factor authentication

Physical security issues

Staff on-going training

When do you foresee the DOD starting assessments?

Many small companies are asking how is this going to be affordable?

Can you speak to what is considered an allowable contract cost?

Thank You!

Roy Luebke
Email: rluebke@genedge.org
Mobile: 276-732-8372

SC CYBERSECURITY SUMMIT

IT Consultant Vendor Panel

Sponsored by:

dew

South Carolina Department of Commerce
Just right for business.

SC MEP
SOUTH CAROLINA MANUFACTURING EXTENSION PARTNERSHIP

Melissa Steinkuhl
Regional Vice President
SC Manufacturing Extension Partnership

Matt Fraser
Director of Business Development
Epsilon, Inc.

Zachary Hodges
VP & Chief Operating Officer
Cyber Security Solutions, Inc.

Wes Knight
CISO/Director – Government Sector
Needling Worldwide

Trenelle Lyiscott
Cytellix Corporation
Cyber Support Manager

Eric Power
Director of Strategic Initiative
BERYLLIUM Infosec Collaborative

Hunter Roark
Vice President of Technology and Services
Cantey Tech Consulting

Ms. Lizzie Tinker CEH, CISSP
Cybersecurity Sr. Manager
Elliott Davis

SC CYBERSECURITY SUMMIT

SC Cap Phase I Experience:

TETRAMER®
MOLECULAR ARCHITECTS

Sponsored by:

dew

South Carolina Department of Commerce
Just right for business.

SC MEP
SOUTH CAROLINA MANUFACTURING EXTENSION PARTNERSHIP

Adam Haldeman
Research and Technology Manager
TETRAMER Technologies, LLC

TETRAMER®

MOLECULAR ARCHITECTS

www.tetramer.com

linkedin.com/company/tetramer

Adam Haldeman

Research and Technology Manager

(and IT Manager/Officer/Technician/Guy)

Adam.Haldeman@Tetramer.com

864.646.6282 x202

Solving Materials Problems: Molecules to Manufacturing

We partner with our customers to determine the desired performance of their product

We put the right atoms in the right places to produce materials with the right properties

We develop and transition those materials from the lab to the market or battlefield.

Industry **Defense/Energy** **New Ventures**

TETRAMER®

Tetramer History

2001
Tetramer founded to manufacture optical polymers for the planar waveguide industry

2003
Tetramer R&D expanded to general advanced materials

2009
Tetramer begins serving the DOD

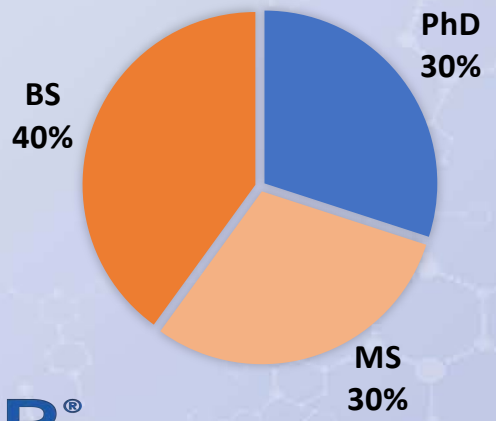
2011
Analytical Lab built out to support R&D efforts

2013
18,000 ft^2 research lab purchased from Clemson University

2017
ISO9001-2015 Certified Quality Management System

2018
Tetramer begins manufacturing and sales of proprietary polyimide polymers.

2021
Tetramer begins manufacturing and sales of VBASE™ base oils and lubricants



TETRAMER®

Research Platforms

Nanocomposite Development
- Tamper-Indicating Coatings
- Radiation Detection
- Phosphor/QDs

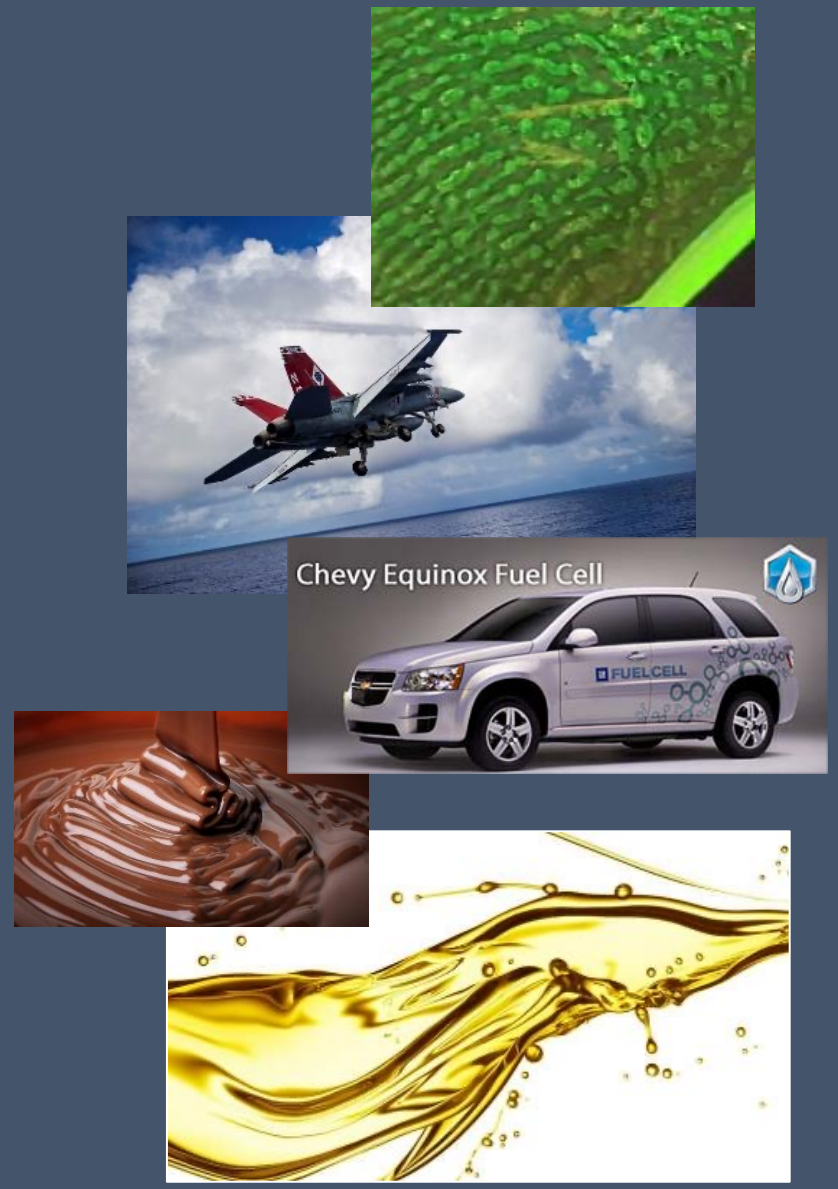
Optical Polymers
- Ultra-low loss optical polymers
- UV curable fiber optic adhesive

Polymers for Fiber Optic Systems
- UV-Curable Index Matching Adhesives
- High Temperature, High NA
- High Temperature for Down-hole

Polymeric Membranes
- Proton Exchange
- Water Vapor Transport
- Electrolyzer
- Gas Separations

Bio-based Lubricants and Oils

Low Calorie Fat Substitutes



TETRAMER®

Manufacturing and Scale-Up

In-House manufacturing & established relationships with toll manufacturers

Expertise in Custom Synthesis and Scale-up

- Development of specifications
- Preliminary cost of manufacture estimations
- Identify and characterize waste streams
- File PMN
- Identify toll manufacturers
- Develop detailed Tech Transfer Packages
- Develop SDS

Full Analytical Laboratory to support production

CMMC Level 3 Compliance anticipated in 2021

Tetramer Quality Management System is ISO 9001:2015 Certified

TETRAMER®

Low-Calorie Fat Replacer

EPOGEE®

Project Description

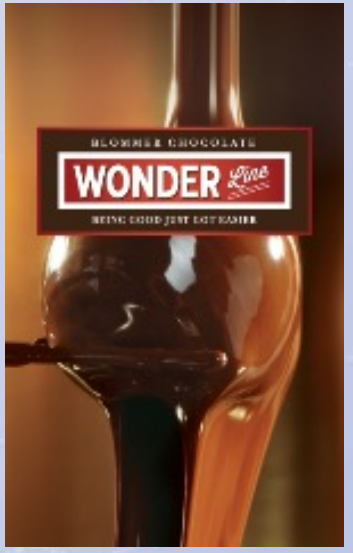
Tetramer Technologies developed Esterified Propoxylated Glycerol (EPG), a fat replacer for calorie and fat reduction in foods with Epogee.

Results

I. Developed EPGs optimized for confectionery and spreadable foods.
II. Demonstrated EPG's scalability through multiple manufacturing-scale runs, resulting in over 500,000 lbs. of EPG manufactured to date.
III. Developed ideal EPG/fat blend formulations for a variety of foods including confectionery coatings and nut spreads.
IV. Currently working with Epogee in technical sales support as well as continued R&D.

Objectives

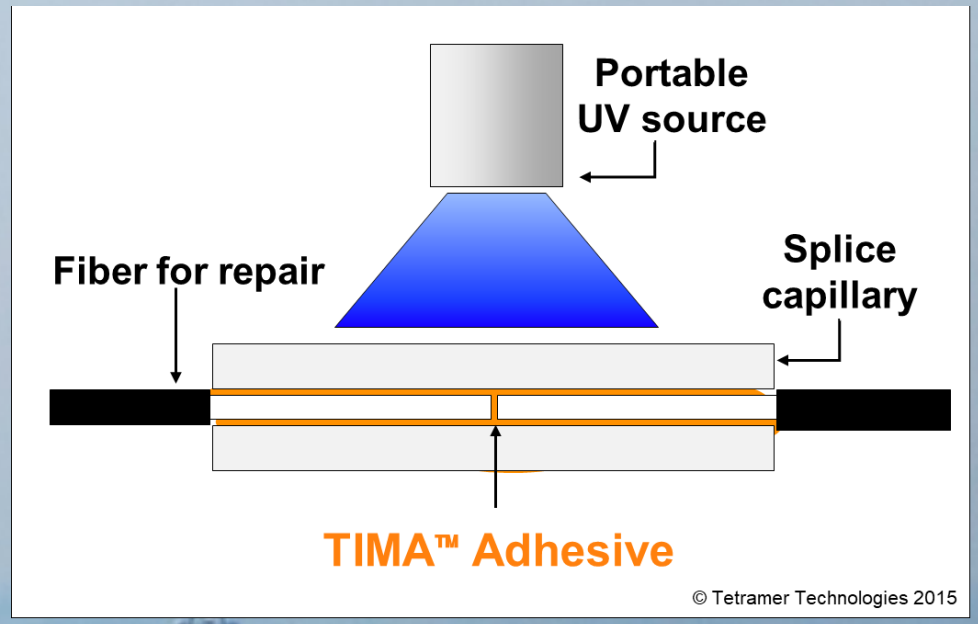
- ✔ I. Develop EPG formula for use as a low-calorie fat replacer in a variety of end-use food products
- ✔ II. Demonstrate effective EPG use in target foods and optimize for potential customers' needs.
- ✔ III. Scale up EPG production to manufacturing scale.
- ✔ IV. Commercialize EPG in food industry.



TETRAMER®

TIMA™ UV-Curable Adhesive

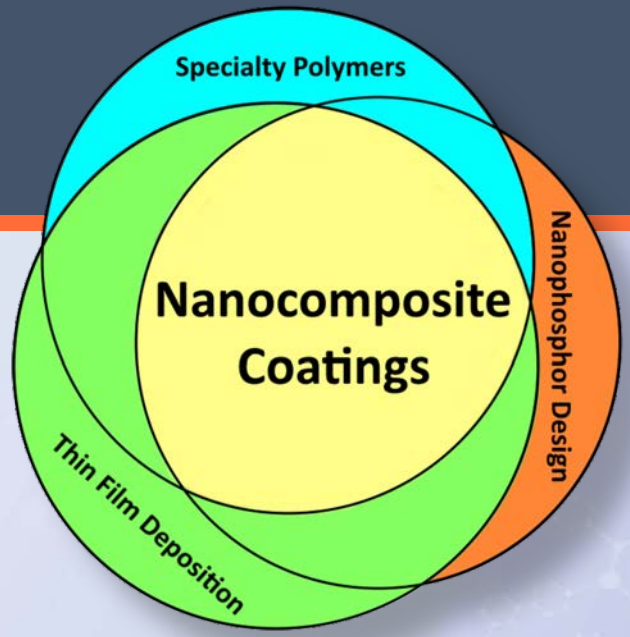
Fixing Navy fighter jets in the field



Works in Extreme Conditions | No Climate Control Needed

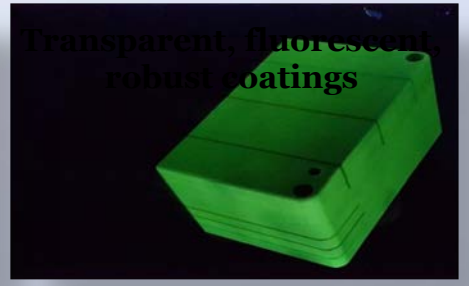
TETRAMER®

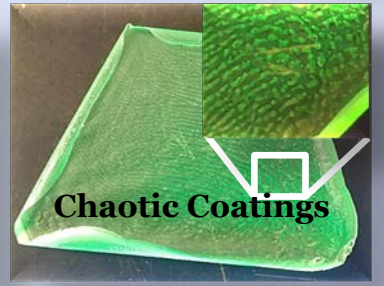
DOE-TIC Phase III

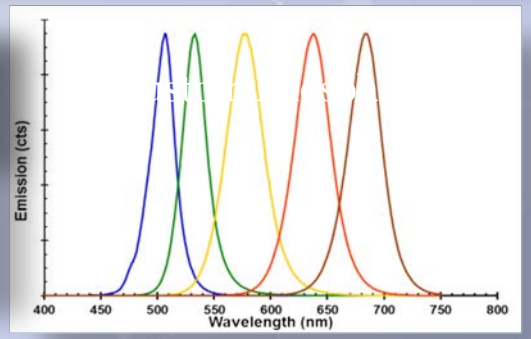


Competencies in the development of advanced nanophosphors, specialty polymers, and thin film deposition techniques have been combined to develop nanocomposite coatings.

- Applications include:
- Intrusion Detection Coatings
- Unique Identification/serialization
- Bulk nanocomposite fabrication
  - Potential for alternative bulk gamma-ray scintillator materials development
- Chaotic/covert coatings







TETRAMER®

Tetramer Cybersecurity

2015

2021 (?)

TETRAMER®

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

- Sun Tzu, The Art of War

TETRAMER®

Why is CMMC important for Tetramer?

- To continue to serve the DoD, the warfighter, and the American citizen.
- To continue supplying existing Tetramer products and services to the DoD – maintaining current business.
- To grasp new opportunities in the DoD supply chain and meet company growth objectives.
- To be ready.

"The readiness is all."

- William Shakespeare

TETRAMER®

SC-CAP Phase I

The Process

- Apply for the Opportunity!!
  - Show letters/contracts and revenue coming from DoD customers supporting your need for CMMC
- Select a Vendor
  - How knowledgeable are they on the CMMC requirements?
  - Do they understand your company's approach and goals for compliance?
  - Who can propel you the farthest toward accomplishing compliance?
- Engage your Vendor
  - Expect a thorough assessment and a well-developed POAM.
- Consistently Work at Remediation
  - Keep going Mr. Tortoise!

TETRAMER®

SC-CAP Phase I

Lessons Learned

- Ask lots of questions and take good notes.
- Don’t underestimate the time and effort needed to fix your IT infrastructure and procedures.
- Communicate with your CEO now. CMMC will require time, money, and knowledge (repeatedly).
- Make sure your CMMC strategy is sustainable for your company.
  - Cost
  - Resource availability (personnel and systems)
  - Who’s actually going to do maintenance, monitoring, reporting, and auditing?

Tetramer Cybersecurity Strategy

- Engaging Beryllium InfoSec for SC-CAP Phase II
- Originally, my strategy was to CMMC-proof all of Tetramer
  - Too burdensome on the company culture
  - Aggregating technology solutions made for a messy security plan and left gaps in monitoring/auditability.
  - I wasn't going to manage it well.
- Changed direction to enclaving DoD users in a compliant environment (CUIck Trac)
- Once our POAM is completed, we will pursue CMMC certification.

If at first you don’t succeed, call it Version 1.0

Adam Haldeman

Research and Technology Manager

Adam.Haldeman@Tetramer.com

864.646.6282 x202

TETRAMER®

Dr. Cynthia Davis
Business & Industry Programs Manager
SC Department of Commerce

SC-Cybersecurity Assistance Program (SC CAP) Phase 2

Overview

- Seeking 31 SC MFRs operating in the DoD Supply Chain
- Total of $25K in services to move the company *towards* CMMC Level 3
- $22K available through SC-CAP grant Phase 2
- $3K to be paid by client
- 7 approved vendors
- Maximum of 9 projects for any one vendor

South Carolina Department of Commerce
Just right for business.

SC-CAP Phase 2

7 Approved Vendors

- Beryllium Sec Info (Minnesota, MN)
- Cantey Technology (N. Charleston, SC)
- Cyber Security Solutions (Augusta, GA/Tampa, FL)
- Cytellix Cybersecurity (Mission Viejo, CA)
- Elliott Davis (Greenville, SC)
- Epsilon (Weaverville, NC/Greenville, SC)
- Needling Worldwide (Greenville, SC/Georgia)

South Carolina Department of Commerce
Just right for business.

SC-Cybersecurity Assistance Program (SC CAP) Phase 2

Project Timeline

- September 1 - October 1 Grant Application Period
- October 2- October 8 Application Review & Scoring
- October 15 Award Notification to Companies
- October 18 Company & IT Consultant Matching by SCMEP
  - Proposals & Invoicing
  - Consultation begins upon receipt of $3K
  - Assessment
  - Technical Assistance

South Carolina Department of Commerce
Just right for business.

SC-CAP Phase 2

Project Deliverables

- Review of client's existing NIST SP 800-171 DoD Self-Assessment and the score generated
- If not previously performed the vendor is assist the client with performing the self-assessment and entering the score in the Supplier Performance Risk System (SPRS)
- Gap assessment
- Develop and then implement a Plan of Action & Milestones (POAM)

South Carolina Department of Commerce
Just right for business.

SC-CAP Phase 2

Project Deliverables

- Develop and implement a System Security Plan (SSP)
- Provide resources to develop policies, procedures, and practices per the 130 CMMC Level 3 controls
- Document Objective Evidence to demonstrate compliance to CMMC Level 3

- Note: SC-CAP grant funds CANNOT be used to cover the purchase, installation, set-up, or commissioning of hardware (servers, firewalls etc.) or software (i.e.Microsoft Office 365)

South Carolina Department of Commerce
Just right for business.

Go to:

scbizdev.sccommerce.com

For the Grant Application

To Complete Evaluations, Check your email:

SC Cybersecurity Summit Survey

Director Dan Ellzey
Executive Director
SC Department of Employment and Workforce

SOUTH CAROLINA DEPARTMENT OF

Employment and Workforce

South Carolina Cybersecurity Summit

Dan Ellzey, Executive Director

- March 5: Noticed that almost 20,000 fraudulently created accounts were established in our unemployment portal.
  - By an unknown actor or group of actors
  - Computer-driven script
  - Security system stopped them from actually filing claims. No claims were filed.
  - No money was paid.

- Had this occurred at the beginning of the pandemic, before we installed the security software, we would've paid out millions of dollars. The State of Washington paid out between $500-700 million in fraudulent claims at the beginning.

- If your company has something that the criminals want and can get online, you will be attacked.
  - In our case, the federal UI benefits were appealing.
  - Defense contractors also have something that people want. For that reason, your systems must be guarded.

- And that is the purpose of this entire program.

Cybersecurity Workforce

- As businesses implement CMMC standards, some may need more specialized workers to develop and maintain the CMMC IT and Cybersecurity safeguards.

Occupation	Statewide Median Wage	Employment
Computer and Information Systems Managers	$121,580	3,460
Computer and Information Research Scientists	$102,060	400
Computer Hardware Engineers	$95,390	490
Computer Network Architects	$86,770	1,010
Software Developers and Software Quality Assurance Analysts and Testers	$85,990	7,790
Database Administrators and Architects	$80,200	920
Information Security Analysts	$80,070	1,630
Computer Systems Analysts	$78,540	7,650
Computer Programmers	$77,290	2,850
Network and Computer Systems Administrators	$73,580	6,100
Computer Science Teachers, Postsecondary	$70,020	370
Computer Network Support Specialists	$53,020	2,250
TOTAL JOBS		34,920

Source: Occupational and Wage Statistics, May 2019

To obtain the needed skills, defense firms can hire people or train existing employees through programs such as Incumbent Worker Training.

- Incumbent Worker Training helps you stay on the cutting edge and increase productivity and quality through providing employees with needed training.
  - Workforce Innovation and Opportunity Act
    - funding available to help off-set some training costs
    - If approved for training assistance, a business is reimbursed for approved training costs
  - CompTIA IWT Program
    - Scholarship opportunities for businesses to train employees in CompTIA A+ or CompTIA Security +
    - Businesses will apply for scholarships to train employees directly with CompTIA
    - More to come.

Call to Action – SCCAP

- Implementing Cybersecurity Maturity Model Certification (CMMC) practices can be a rigorous process.
  - The technical assistance being offered through the SC Cybersecurity Assistance Program will help significantly.

- The State of South Carolina values your company and the contribution you make to our state. We want you to be successful. We want you to continue performing and growing the number of defense contracts you have in South Carolina.
  - Let us know what we can do to help.

- Any questions or needs you may have regarding worker recruitment and reskilling, contact Nina Staggers at nstaggers@dew.sc.gov.

SC CYBERSECURITY SUMMIT

Thank you for attending today
&
Safe travels!

Sponsored by:

dew

South Carolina Department of Commerce
Just right for business.

SC MEP
SOUTH CAROLINA MANUFACTURING EXTENSION PARTNERSHIP