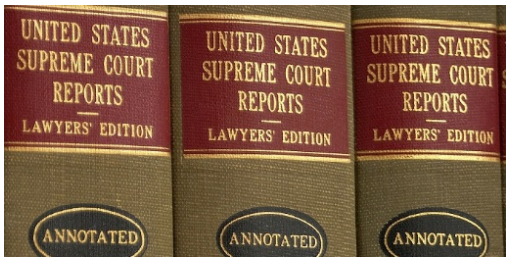
SUFFOLK ACADEMY OF LAW

The Educational Arm of the Suffolk County Bar Association

560 Wheeler Road, Hauppauge, NY 11788

(631) 234-5588



ZOOM PROGRAM

WORKING REMOTELY: CYBERSECURITY ISSUES & CONCERNS

FACULTY

Michael Stanton, Esq.
Joseph Bucco
Mitchell T. Borkowsky, Esq.

September 17, 2020
Suffolk County Bar Association, New York

Like us on:

"The opinions, beliefs and viewpoints expressed herein are those of the authors and do not necessarily reflect the official policy, position or opinion of the Suffolk County Bar Association, Suffolk Academy of Law, their i Board of Directors or any of their members"

Joseph Bucco

I've been involved with IT security for most of my professional life. I've worked in banking, healthcare, and now in the managed services sector totaling 14 years of IT security experience. I started my career with a local bank as a data security consultant, and then went on to build the cybersecurity program at a long island hospital from the ground up. I've been at Stafford Associates for 3 years now, where I get to architect security solutions and strategies for a wide variety of clients of all sizes across a wide variety of industries. I absolutely love working in the field as I get to continually learn and am always being exposed to cutting edge and emerging technologies. I love having opportunities to speak and raise general awareness about cybercrime and how to keep safe in today's constantly evolving digital and interconnected world.

Michael Stanton, Esq.

"Mike Stanton is an attorney with Sinnreich Kosakoff & Messina LLP in Central Islip, New York. He has extensive experience in litigation and appeals, including defense of architects and engineers, municipal defense, and commercial litigation. Mike is expanding his practice to include cybersecurity, privacy, and data protection, including litigation and compliance with newly-developing laws and regulations."

Mitchell T. Borkowsky, Esq. is the former Chief Counsel to the New York State Grievance Committee for the Tenth Judicial District of the Supreme Court, Appellate Division, Second Department.

For over twenty years, Mr. Borkowsky ascended the ranks of the Grievance Committee's professional staff, rising from financial auditor to staff counsel to Deputy Chief Counsel and, finally, Chief Counsel. During his tenure with the disciplinary authorities, Mr. Borkowsky conducted, or was involved in, thousands of investigations and prosecutions of complaints alleging ethical or professional misconduct by attorneys. Mr. Borkowsky also worked in the Attorney Matters Division of the Law Department at the Appellate Division, Second Department, where he reported to the Justices of that court on attorney disciplinary and reinstatement proceedings and drafted disciplinary decisions. In that capacity, Mr. Borkowsky observed, first-hand, the seriousness and deliberate manner in which the Justices and their staff report on, and decide, disciplinary, admissions, and reinstatement matters.

As Chief Counsel and Deputy Chief Counsel to the Grievance Committee for eleven years, Mr. Borkowsky provided legal advice and guidance to the Committee, its chairpersons, and its individual members, while overseeing the operations of the Committee's professional and administrative staff. He reviewed and made determinations concerning the merits of just about every grievance complaint filed with the Grievance Committee and every report or pleading generated by the staff, while at all times maintaining his own caseload of complex matters.

Prior to joining the staff of the Grievance Committee, Mr. Borkowsky engaged in the general practice of law for both small and large firms, and as a solo practitioner concentrating in the areas of real estate and commercial transactions, general litigation, and trusts and estates. As a practitioner, Mr. Borkowsky handled many of the same kinds of legal matters and issues giving rise to the majority of grievance complaints filed by clients and others.

In addition to disciplinary and general legal work, Mr. Borkowsky has represented individuals suffering from mental health issues and assisted families in guardianship proceedings before the Supreme and Surrogate's Courts, pursuant to Article 81 of the Mental Health Law and Article 17-A of the Surrogate's Court Procedure's Act. With lawyers under more stress than ever, the profession's mental health has become the focus of increasing concern, as evidenced by numerous articles and bar association initiatives combatting depression and substance abuse. Through his personal and professional experiences, Mr. Borkowsky has a keen understanding of the effects that stress and family crises can have on a lawyer's well-being.

Mr. Borkowsky was admitted to practice in May 1994, having received his Juris Doctorate from Brooklyn Law School. Prior to attending law school, Mr. Borkowsky worked as an accountant/auditor for a large New York City public accounting firm and as a mortgage loan originator for a major New York lending institution.

Mr. Borkowky has taught courses at Hofstra University and at the Real Estate Training Center of Greater New York, and regularly lectures on attorney ethics and disciplinary matters at various Continuing Legal Education programs sponsored by the Nassau, Suffolk, and New York State Bar Associations, local law schools, and other venues.

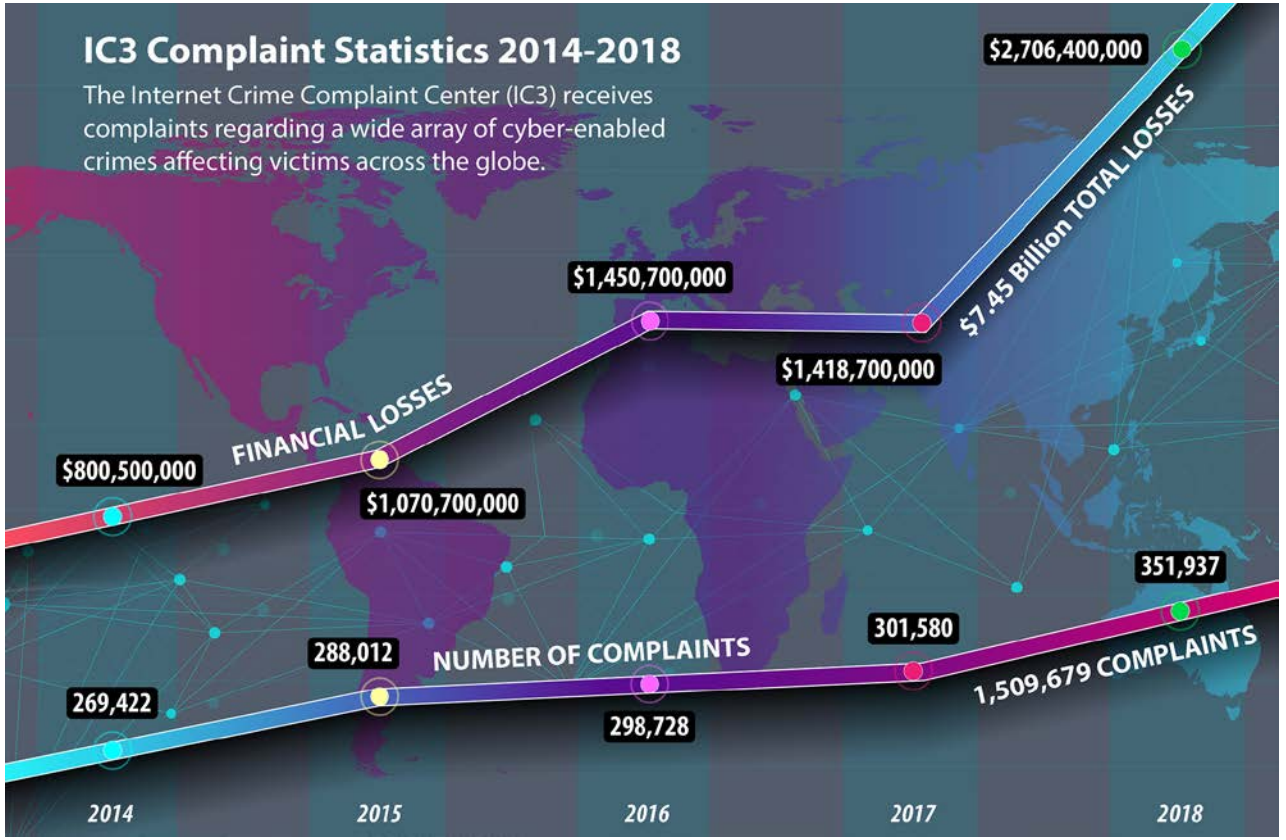
Stafford ASSOCIATES

COMPUTER SPECIALISTS INCORPORATED

Cybersecurity Educational Workshop

Cyber Crime

Now a reality of the digital age



Stafford ASSOCIATES

COMPUTER SPECIALISTS INCORPORATED

Narrowing the Focus

- Managing your internet presence
- Technical controls and security best practices
- Security while working remotely
- Security when using online meeting tools
- Security as a separate thought process

Managing Your Internet Presence

- Most companies have little to no idea what information they have publicly available on the web

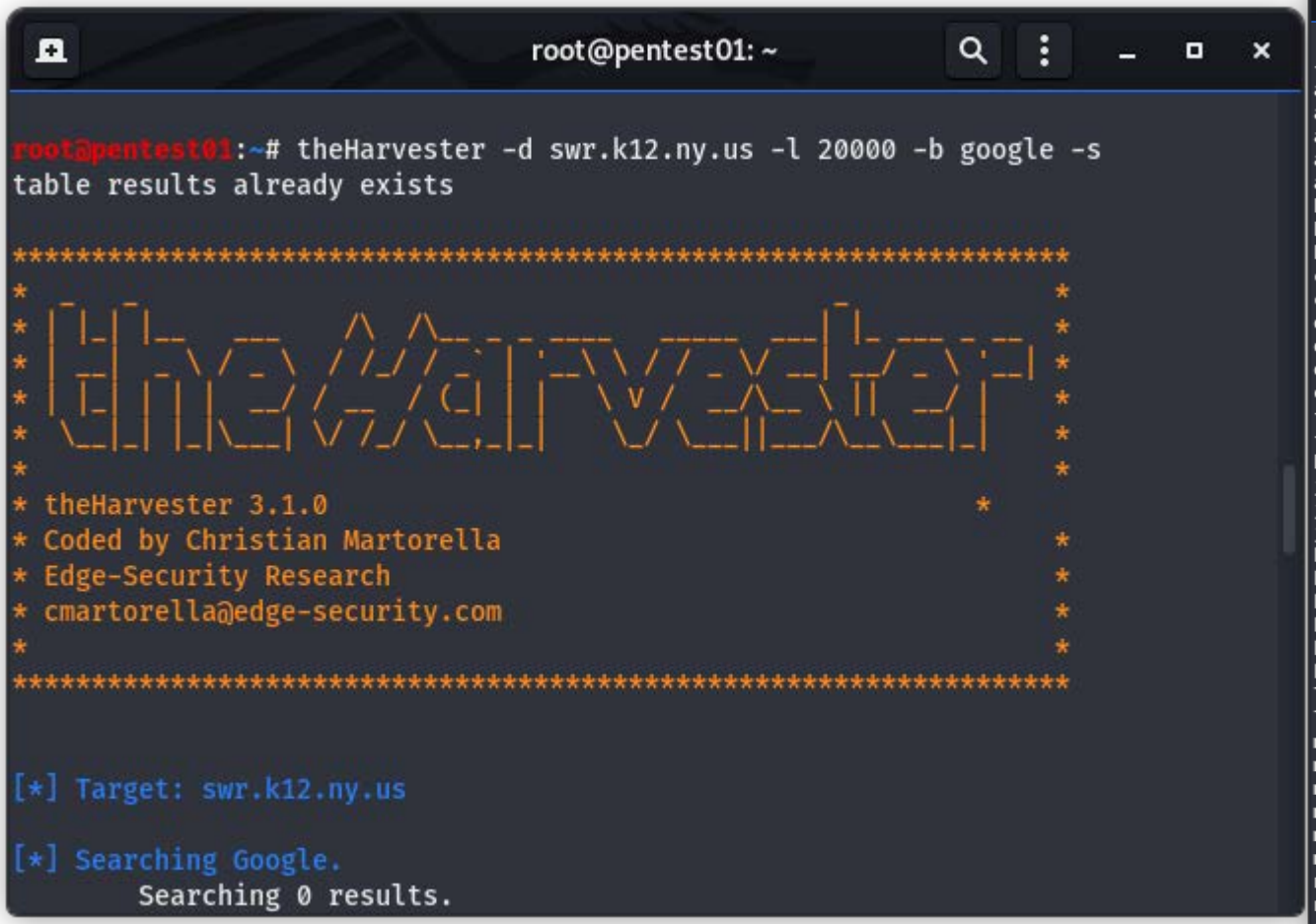
- Most companies also have little to no idea how that information can be used against them

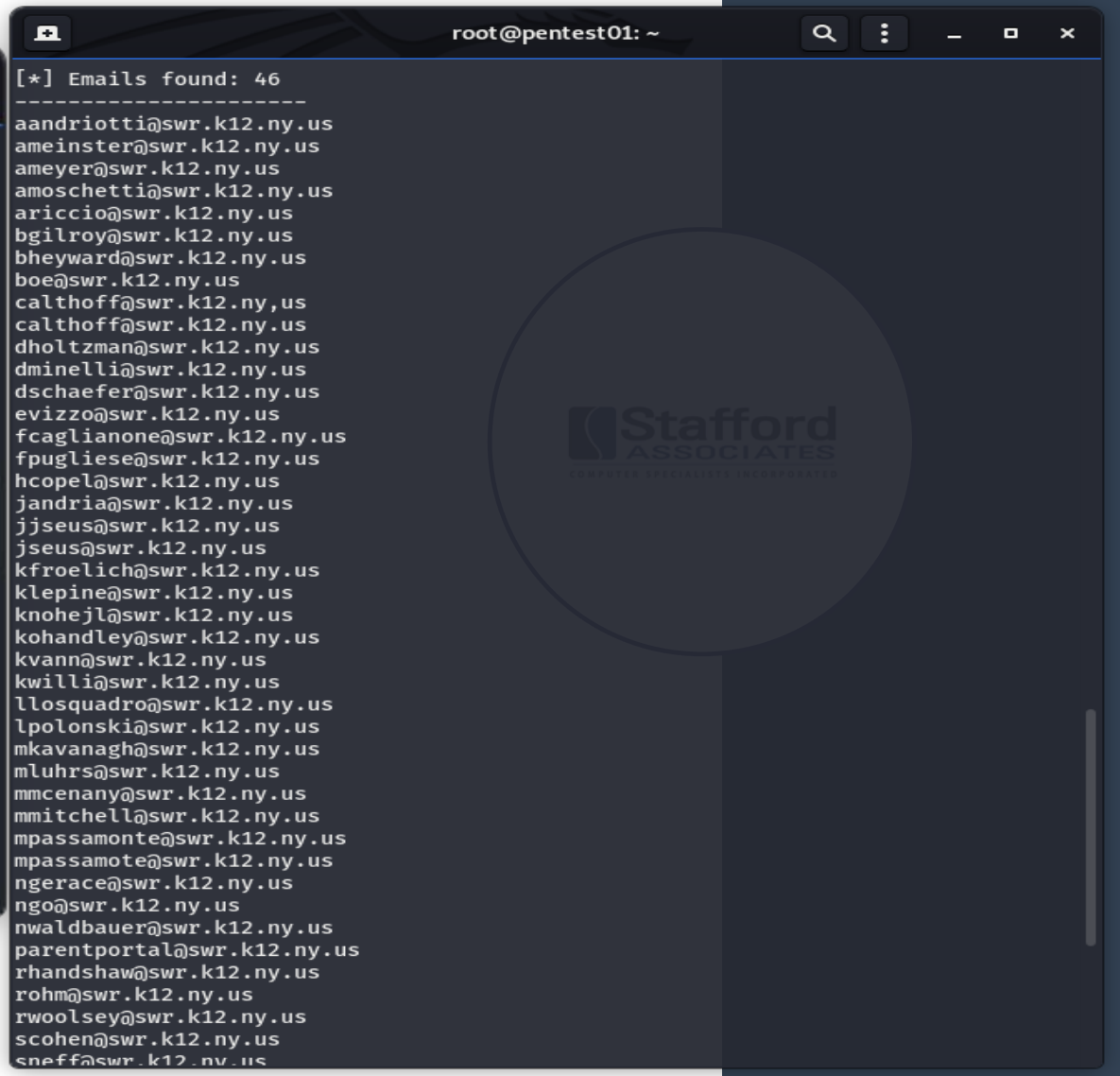
Managing Your Internet Presence

- Limit any personally identifiable, sensitive, or otherwise non-public information on the web

Here's Why:

Managing Your Internet Presence





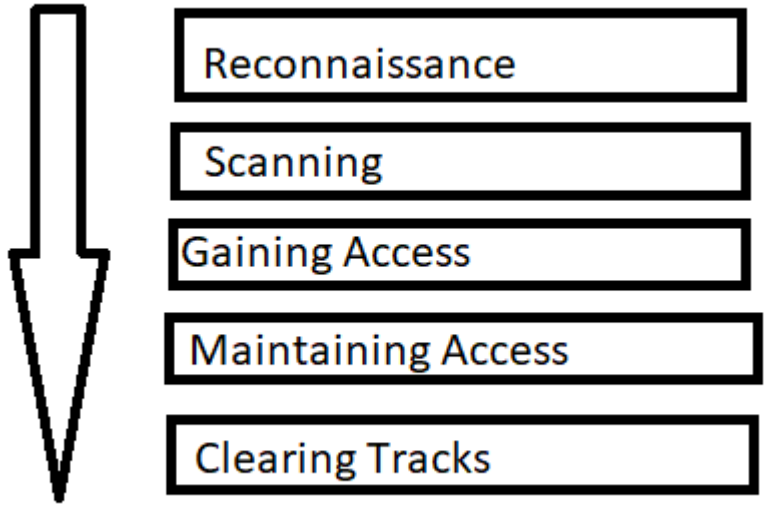
Managing Your Internet Presence

So what? What can a hacker do with my email address?

- I now have 46 potential targets for phishing attacks
- I can find these individuals online through social media or other means, and gather all personal information I can to further tailor my attacks, increasing likeliness of success
- If I gain access to any devices at the target company, I now have personal information and keywords to feed my automated password cracking tools which I would then use to move laterally through the network and further establish my foothold

Stafford ASSOCIATES
COMPUTER SPECIALISTS INCORPORATED

Phases of a Hack



- Up to 95% of the time spent on a hack could potentially be attributed to target reconnaissance

Types of Attackers

Script Kiddie

- Most likely to come across
- Someone who uses existing exploits and scripts/code to perform hacks
- Cannot write their own exploits / code because of lack of skill
- Still very dangerous

Insider Threat

- Not as likely as script kiddie, but more likely than APT
- Very dangerous as they already have inside access
- Around 34% of data breaches in 2019 were caused by an insider attack

APT (Advanced Persistent Threat)

- Least likely to come across
- Highly skilled and adaptable
- Usually has specific objective
- Well funded
- Could possibly be state sponsored

Stafford ASSOCIATES
COMPUTER SPECIALISTS INCORPORATED

Technical Controls & Security Best Practices

- Keep software up to date
  - Operating Systems
  - Third Party Applications
  - Browsers
- Regularly back-up important data
- Due diligence for all third parties / vendors
- Use commercially supported endpoint protection
- Institute the principle of least privilege / control use of administrative privilege
- Manage vulnerabilities
- Inventory and control of hardware assets
- Control physical access to facilities and information
- Enforce safe password practices
- Securely destroy / sanitize all media

Stafford ASSOCIATES
COMPUTER SPECIALISTS INCORPORATED

Technical Controls & Security Best Practices

- Educate Employees
  - How to spot a malicious email
  - Using good browsing practices
  - Avoiding suspicious downloads
  - Creating strong passwords
  - Protecting sensitive customer and vendor information
- Use a firewall
- Use MFA where possible
- Write and document a cybersecurity policy or set of policies
- Encrypt mobile devices
- Separation of duties
- Have an incident response plan for when something does happen!!!!!!

Stafford ASSOCIATES
COMPUTER SPECIALISTS INCORPORATED

Stay Secure While Working Remotely

- Only use trusted and encrypted wireless when not at the office (ideally all work network traffic should be secured by a corporate VPN)
- Use MFA wherever it is possible/feasible
- Use a legitimate password manager to help secure passwords, and create secure passwords
- Never leave work equipment unattended
- Company issued devices should be used for WORK ONLY
- Change your router login and password from vendor defaults
- Lock/secure your device before walking away
- Always use corporate accounts for mail, messaging, and all other things that are business related

Stafford ASSOCIATES
COMPUTER SPECIALISTS INCORPORATED

Security When Using Online Meeting Tools

- Secure online meetings with pins / passwords
- Do not reuse access codes / passwords often
- Use MFA if offered
- Use a waiting or lobby area and don’t allow meeting to begin until the host joins
- Enable notification when attendees join, such as playing a tone or announcing names. If this is not an option, make sure the meeting host asks new attendees to identify themselves
- If available, use a dashboard to monitor meeting attendees
- Don’t record the meeting unless necessary
- Disable features that are not needed – ie: chat, file sharing

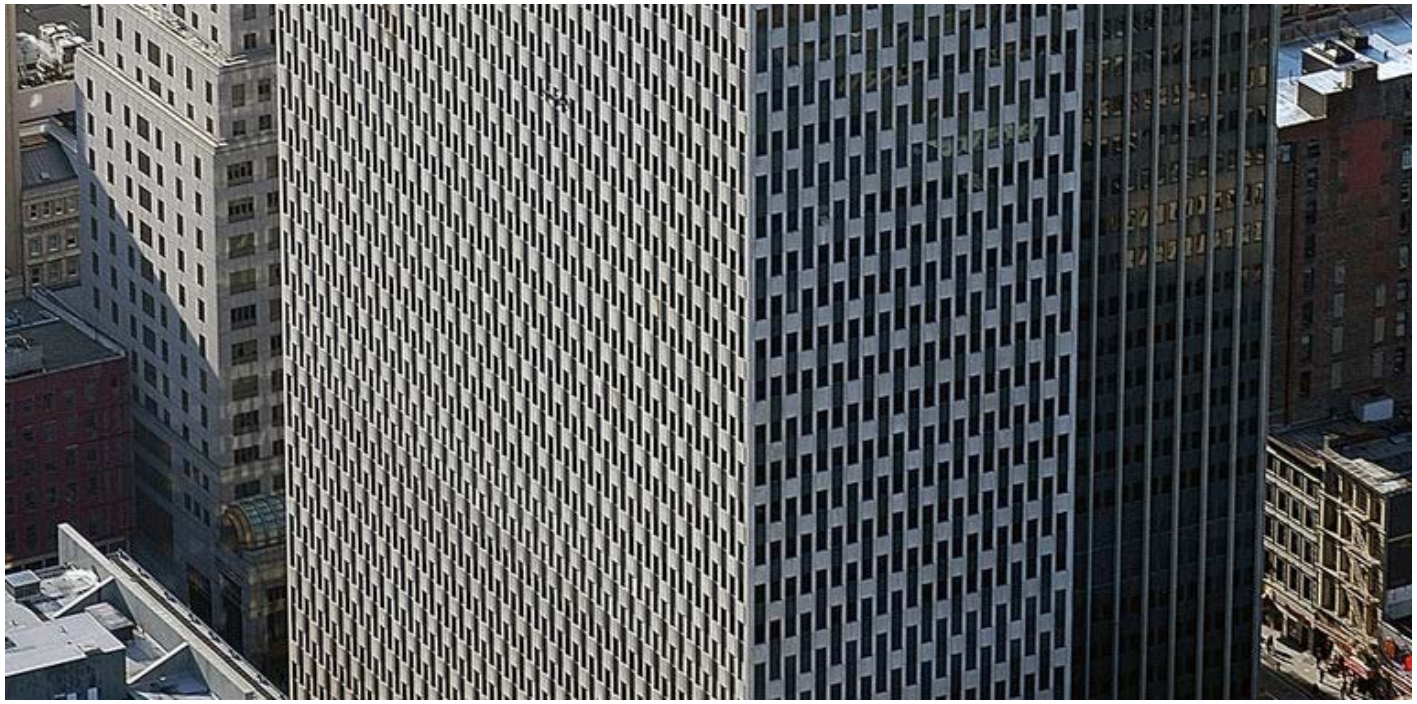
Zoom Specific Security Measures

- Always use the latest version of the zoom app
- Password protect meetings
- Allow only signed in users to participate in meetings
- Do not allow attendees to join before the host
- Turn off participant screen sharing
- Lock the meeting as soon as all participants have joined
- Use a randomly generated meeting-id
- Use the waiting room feature to screen participants upon entry
- Avoid file sharing

Security as a Separate Thought Process

- General IT and IT Security should be distinctly separate entities in larger organizations
- If you have limited IT staff with limited security expertise, reach out to a reputable consultant or managed services provider
- Make sure you are practicing “Defense-in-Depth” to the fullest extent possible
- Know your vulnerabilities and security pain points
- Think of the security implications of all business or IT related decisions
- Know what to do if you are breached
  - Know who to contact if you are breached
  - Know your reporting obligations if you are breached
  - Know what remedial actions need to be taken if you are breached
- Do not become complacent, it is no longer a matter of if, but when!

Your Local FBI Field Office



New York
26 Federal Plaza, 23rd Floor
New York, NY 10278-0004
newyork.fbi.gov
(212) 384-1000
Covers the five boroughs of New York City, eight counties in New York state, and La Guardia Airport and John F. Kennedy International Airport

Stafford ASSOCIATES
COMPUTER SPECIALISTS INCORPORATED

IT Security Services offered by Stafford Associates

- Defense in Depth Strategies – Tailored for your Business
- Network and Firewall Monitoring
- Audit and Compliance Support
- Comprehensive Endpoint Protection
- Workstation and Server Environment Hardening
- Managed Workstation and Server Plans
- Managed Patching for Managed Workstations and Servers

Questions?

Joseph Bucco
Sr. IT Security Engineer
jbucco@staffordassociates.com
P: (631)-751-6620
M: (631)-579-8862