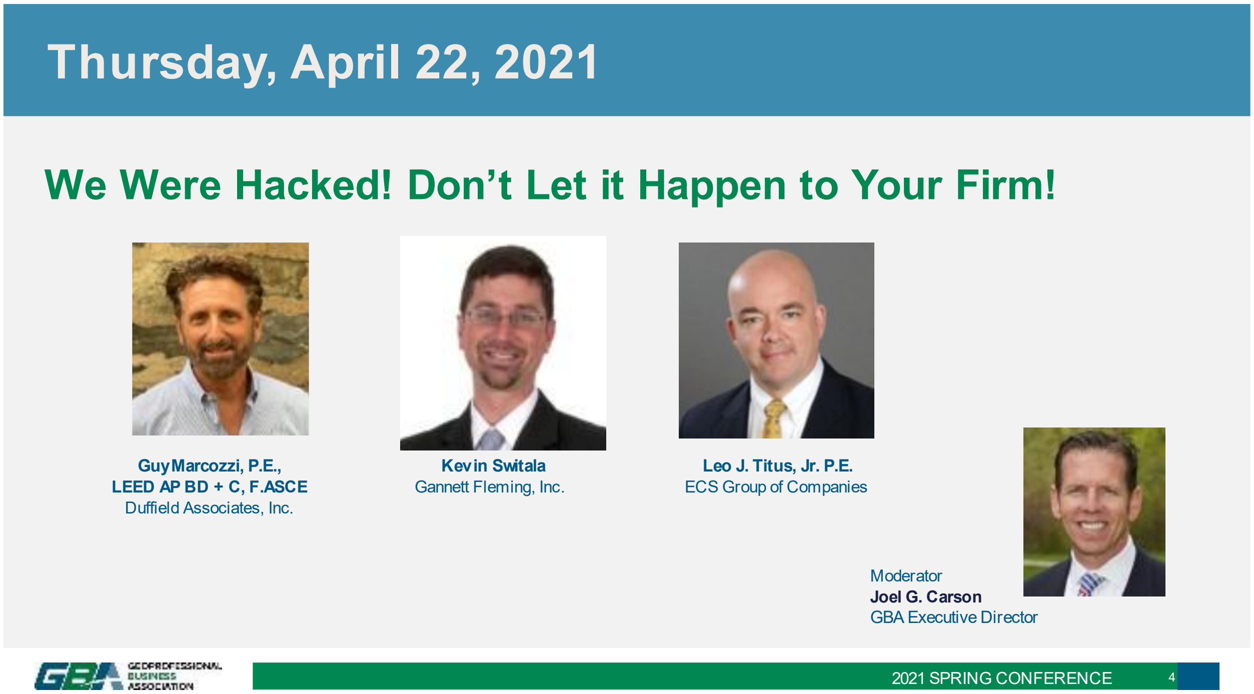

Thursday, April 22, 2021

We Were Hacked! Don't Let it Happen to Your Firm!

Guy Marcozzi, P.E., LEED AP BD + C, F.ASCE
Duffield Associates, Inc.

Kevin Switala
Gannett Fleming, Inc.

Leo J. Titus, Jr. P.E.
ECS Group of Companies

Moderator
Joel G. Carson
GBA Executive Director

GEOPROFESSIONAL BUSINESS ASSOCIATION

2021 SPRING CONFERENCE 4

Questions /Answers (after session concluded)

1. **Does the future look like fully going to cloud-based computing and cloud-based systems to specifically mitigate these hacker attacks?**

   Kevin (Gannett Fleming)
   It is important to remember that digitally transforming our collective organizations and migrating data and services to cloud platforms only changes the threat landscape. It does not diminish the threat landscape nor each of our organization's threat profile. It is incumbent upon us to ensure that the cloud platform vendors and those vendors offering us -as-a-Service solutions (SaaS, PaaS, IaaS) are properly securing their environments and systems against attack and compromise (e.g. SolarWinds). A shift to cloud computing and systems just forces us to adjust how we need to creatively envision new routes of compromise by threat actors and to mitigate and defend ourselves in new ways.

2. **Guy, Why did insurance only pay for one day of lost productivity?**

   Guy (Duffield Associates)
   We had some discussion of what "shut down" was and they ultimately concluded that we were only technically shut down for one day. We had to submit quite a bit of documentation to establish that. The reality is people came up with the own work arounds to keep projects moving so they had a point. Perhaps we could have argued harder but we were ready to move on.

3. **If you could go back before this happened, knowing what you know now, what are the three most important things you would do or put in place - software/equipment updates, hire service providers, change processes, staff training?**

   Kevin (Gannett Fleming) – 1. Deploy truly immutable backup capabilities for our large data storage environment and our virtual environment 2. Meet with our Incident Recovery consultant team to provide access to and review existing network, systems, and business process documentation (including DR plans) so that if/when we call upon them to respond to an incident we don't have to spend time briefing them 3. Better enforcement of data archiving policies so dramatically reduce the data being stored within our enterprise, 70% of which will likely never be needed in the future.

Guy (Duffield Associates) – More employee training of the risks. We did more backend work to bolster our security and increase the backup frequency and separation.

Leo (ECS) - 1. Updated hardware/software. 2. Better backup system 3. A more robust security/containment program (which we have now!)

4. **Assuming this could happen again, what "lessons learned" did you incorporate into future cyber-risk planning and/or disaster recovery? Although cyber is different field, geoprofessionals are well-suited to handle stressful disaster type situations!**

   Kevin (Gannett Fleming) – Exercise enterprise business continuity and disaster recovery plans, not compartmentalized just within executive functions, operations, and IT separately, but cooperatively and collaboratively.

   Guy (Duffield Associates) - Second that!

   Leo (ECS) Developed a more coordinated disaster recovery plan to include “emergency kits” in each office including computers that are not on our network loaded with critical tools/forms/programs/etc.

5. **It sounds like file servers were the main point of attack? If so, would cloud-hosted file services have mitigated the attack? Were other on-premise systems (database servers, application servers) affected?**

   Kevin (Gannett Fleming) – Yes, on-network file servers and virtualized environments appear to be favored targets of threat actors. We are aggressively modernizing processes and workflows to leverage cloud-platforms for office productivity and administrative activities (Microsoft O365), design & engineering platforms (BIM360, ProjectWise Connect), construction management (Procore) and various back-office/Share Services platforms (HCM, ERP, LMS) greatly reducing the amount of data we need to manage using on-premise storage.

6. **Would you recommend cyber-insurance? If so, would you consider it expensive relative to the hack impacts? Cheap?**

   Kevin (Gannett Fleming) – Absolutely recommended. The cost of the cyber-insurance cumulatively over several years is still insignificant to the costs associated with recovering from a large-scale attack.

   Guy (Duffield Associates) 100% Agree

   Leo (ECS) - YES!! The cost is nothing compared to the loss of revenue, ransom costs, consultant involvement, etc.

7. **Were any PC's used remotely by your staff impacted by the breach, and how did you deal with that if they were?**

   Kevin (Gannett Fleming) – The ransomware attack propagated encryption services throughout our network. Devices connected to our network, or synching local files with server or network file systems there were encrypted also ended up with encrypted files on their hard drives. We engaged one of our Incident Recovery vendors to build a self-service file decryption ShareFile site. This enabled staff to upload encrypted files they discovered on their hard drives to a secure ShareFile site. Our IR vendor pulled those encrypted files into their secure environment, ran them through the decryption service, scanned the files for residual malicious files and content, then posted the decrypted, clean files back to the ShareFile site for the users to retrieve. This allowed us to establish a multi-channel decryption operation at scale. Simultaneous to this decryption process, we rebuilt ever PC using a clean, hardened image so that we could ensure that the clean data was being loaded back onto a clean PC.

Guy (Duffield Associates) - They ultimately were not, but we brought them all in and scrubbed them before we would allow them to reconnect to our network. In the process we found we had many devices that were not in use and we have a more complete and accurate inventory.

Leo (ECS) - If a remote computer connected to our system remotely it was impacted.

8. **Did the three companies have training in place for all employees incorporating a program to test potential vulnerabilities through our people?**

   Kevin (Gannett Fleming) – We had a relatively immature cybersecurity awareness program underway that has since been enhanced by a robust cybersecurity awareness and training program including recurring simulated phishing attacks, quarterly mandatory cybersecurity education, quarterly awareness emails, annual network penetration testing.

   Guy (Duffield Associates) – Kevin's response is appropriate for our situation as well.

   Leo (ECS) - We had basic training and testing for vulnerabilities, but clearly wasn't as robust as it needed to be.

9. **Who did (or should) you contact 1st? Local Police? FBI? DHS/CISA?**

   Kevin (Gannett Fleming) – We had an established relationship in place prior to the attack with the FBI and they were our first call.

   Guy (Duffield Associates) -We called the police to report it and they referred it to the FBI

   Leo (ECS) I believe the first call was to the FBI.