Data Security for Home Builders

Protecting Your Construction Investment from Catastrophic Loss

Philip R. Stein
305-350-7220
pstein@bilzin.com

Bilzin Sumberg
1450 Brickell Avenue, 23rd Floor
Miami, Florida 33131
Bilzin.com

Why Focus on Data Security at all?

- **Your Project May Be a High-Value Target. The valuable information associated with it includes:**
  - Project Documents Stored on Computer Systems or Shared by Email
  - Sensitive Financial Information for Project Financing
  - Employee Personal Information
  - Drones and Other Project Essentials from the Internet of Things

The Nightmare Scenarios of Construction Data Incidents

- **Infiltration from malicious actors can lead to:**
  - Encryption of project data to render it inaccessible until funds are paid to the hacker (ransomware)
  - Theft of sensitive information such as financial account numbers
  - Redirection of wire transfers for payments intended for subcontractors, suppliers and vendors

The Nightmare Scenarios of Construction Data Incidents (cont.)

- **Infiltration from malicious actors can lead to disaster**
    - Manipulation of drawings or BIM modeling to create delays, latent defects or threaten bodily injury to workers on site
    - Commandeering of connected devices in the Internet of Things such as drones or cranes

Yes, It is Possible to Hack Construction Equipment!

Forbes

42,808 views | Jan 15, 2019, 08:00am EST

Exclusive: Hackers Take Control Of Giant Construction Cranes

Thomas Brewster Forbes Staff

Cybersecurity

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Bilzin Sumberg

Yes, It is Possible to Hack Construction Equipment! (cont.)

Forbes

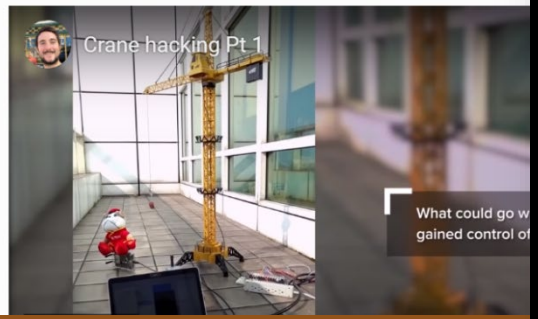
42,808 views | Jan 15, 2019, 08:00am EST

Exclusive: Hackers Take
Of Giant Construction C

Thomas Brewster Forbes Staff

Cybersecurity

Associate editor at Forbes, covering cybercrime, privacy, security



Federico Maggi will never forget the first time he saw a crane being hacked.

Last March, he was on a strange kind of road trip. Travelling the Lombardi region of Italy with his colleague Marco Balduzzi in a red Volkswagen Polo, the pair hoped to convince construction site managers, who they'd never met or spoken with before, to let them have a crack at taking control of cranes with their hacking tools.

Surprise, surprise: They weren't having much luck. But one such manager, who Maggi fondly remembers as Matteo, was game. Armed with laptops powered by the VW's battery, scripts for running their hacks and some radio hardware to beam out the exploit code, Maggi and Balduzzi got to work.

Matteo was asked to turn off his transmitter, the only one on-site capable of controlling the crane, and put the vehicle into a "stop" state. The hackers ran their script. Seconds later, a harsh beeping announced the crane was about to move. And then it did, shifting from side to side. Looking up at the mechanism below a wide blue sky, Matteo was at first confused.

HOW DO HACKERS GET INTO YOUR PROJECT DATA?

The Four Most Common Entries for Hackers

- **Social Engineering**

They are watching your marketing posts, or other published materials, to dig up information on your projects

The Four Most Common Entries for Hackers (cont.)

- **Weak Passwords**
- These are the cause of 80% of cybercrime incidents
- 50% of people use the same password for ALL logins
- The most common passwords, even now, are still:
  - Password (yes, really)
  - [yourname][year of birth]

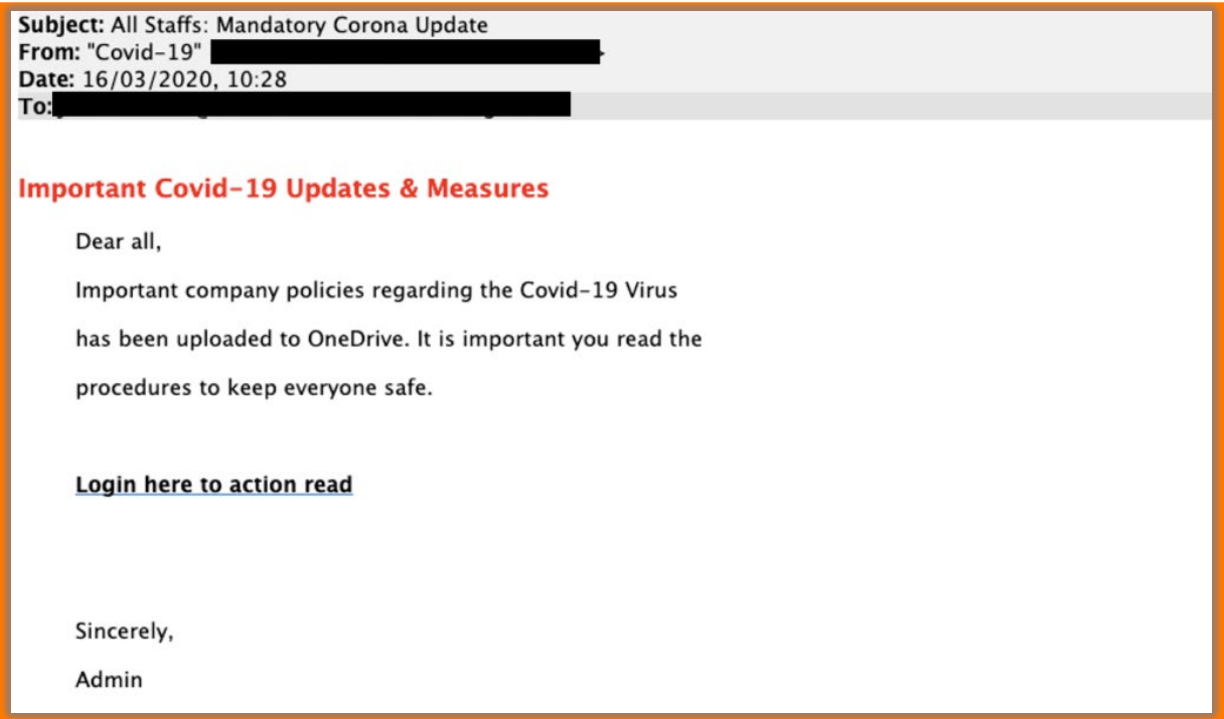
The Four Most Common Entries for Hackers (cont.)

- **Phishing/Spear-Phishing Emails**

- Designed to look like regular emails from trusted or known senders, but will ask recipients to click on malicious links or redirect recipients to enter credentials for login theft

- This is **prime time** for phishing/spear-phishing emails - the holiday season and COVID-19 are creating the perfect storm of traps for the unwary

Recent Infamous Phishing Emails



Subject: All Staffs: Mandatory Corona Update
From: "Covid-19" [redacted]
Date: 16/03/2020, 10:28
To: [redacted]

Important Covid-19 Updates & Measures

Dear all,

Important company policies regarding the Covid-19 Virus has been uploaded to OneDrive. It is important you read the procedures to keep everyone safe.

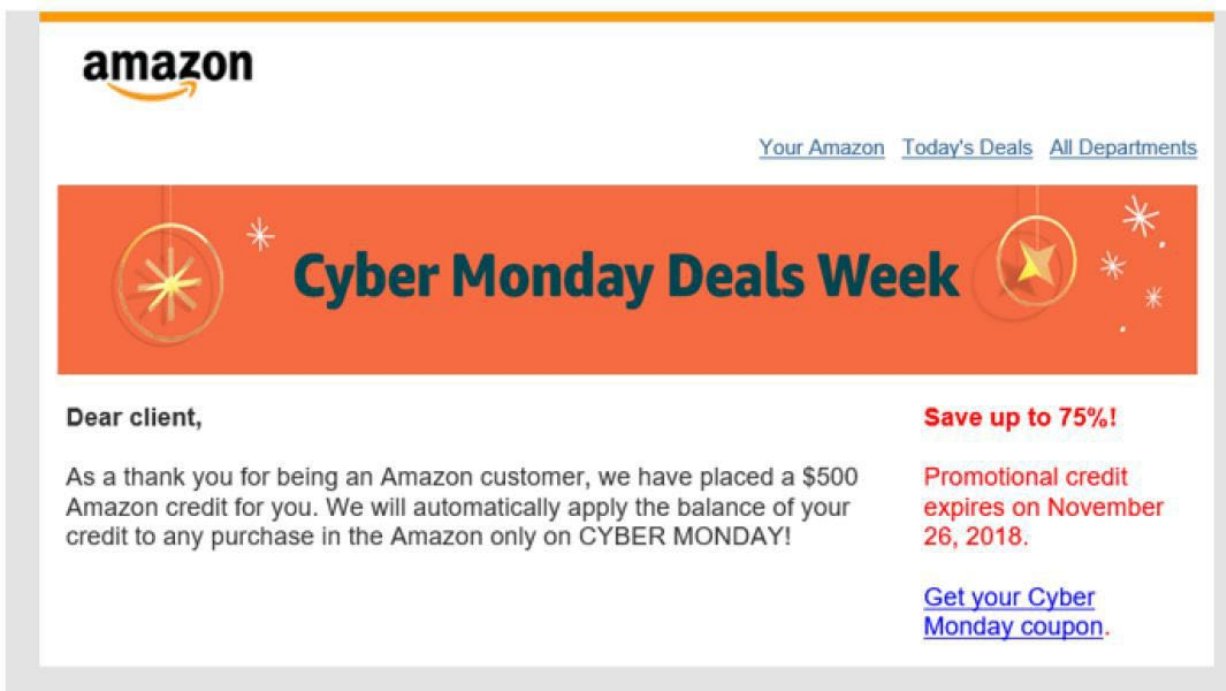
Login here to action read

Sincerely,

Admin

Bilzin Sumberg

Recent Infamous Phishing Emails (cont.d)



The Four Most Common Entries for Hackers (cont.)

- **Malware Attacks**

- Can be the result of clicking on those links we just went over in phishing emails.

- Can also result from connecting a USB or infected smart phone into a laptop connected to your network

- Can also result from downloading unsolicited documents such as PDFs or DocuSign documents

The End Result of These Attacks - Chaos

- **Ransomware Attacks**

- Once a hacker is in your network, or in the Cloud project management software, the hacker can encrypt, rewrite the encryption, on your entire Project file, rendering it useless or inaccessible to you unless you pay.

- The higher the profile of your project or your company, the higher the ransom demand will be. Hackers have studied you. They know their targets.

The End Result of These Attacks - Chaos & Delay

- **Ransomware Attacks - Project Delays**

- The average downtime to your data and information is 17 days in 2020. That's up from 12.1 days in 2019.

- If all of your project data is centralized on a CMiC or Procore-type program, how will a 17-day delay affect the critical path of your project?

- What are the real-world, practical ripple effects of a 17-day delay just to recover project data?

Cautionary Tales from the Construction World

- January 2020 - **Bird Construction** - Ransomware attack involved theft of 60 GB of employees' private information

- Bird has not admitted publicly whether it paid ransom demand from hacker group or whether hackers got information related to Canadian military contracts

Cautionary Tales from the Construction World (cont.d)

Ryuk ransomware hits Fortune 500 company EMCOR

Company expects the incident to have an impact on its 2020 earnings, according to its 2019 Q4 financial report.

- March 2020 - EMCOR - Engineering and industrial construction giant reveals ransomware takedown of several of its IT systems
- EMCOR has also not admitted publicly whether it paid ransom demand

How Can You Mitigate Risks of Attacks?

- **Train your employees in cybersecurity. At a minimum:**
  - How to recognize phishing emails
  - What to do with unsolicited emails, links in emails or document attachments

- **Implement a strong password policy**
  - Prohibit the use of the same login credentials for your company for any other employee device or account
  - Require strong passwords changed regularly

How Can You Mitigate Risks of Attacks? (cont.)

- **Always update your network's security with patches or other updates that your software providers send to you. Do not ignore these.**
- **Use endpoint security to prevent influx of malicious emails.**
- **Back up your data regularly.**
  - Work with your IT professionals or a vendor to have a backup solution not connected to your network, offsite, or on another server entirely. This can neutralize ransom demands.

How Can You Mitigate Risks of Attacks? (cont.)

- Have a detailed written Incident Response Plan, and keep hard copies of it stored securely in addition to electronic copies
- Engage an IT vendor to perform a risk assessment for your company and to identify threats or to sweep for suspicious files in your network
- If you must share important documents by email, encrypt them first and send the password separately or provide it over the phone

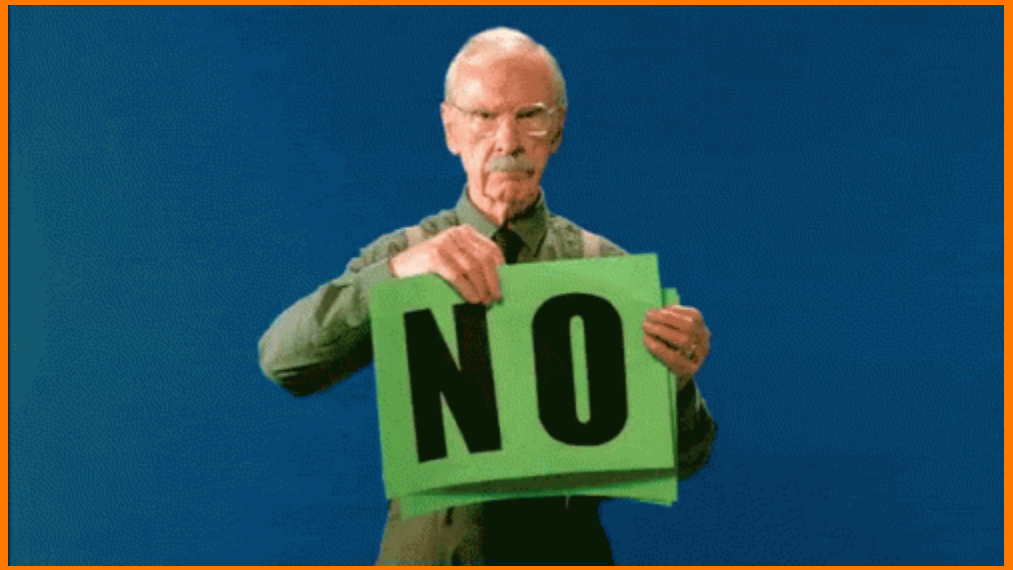
But What About Centralized Cloud Data Storage?

- **Ask these questions of contractors before agreeing to use the contractor's centralized Cloud data storage:**
  - What are the data security protocols in place for the Cloud-based platform through the provider and in contractor's environment?
  - Who at the contractor's business has access to the Cloud-based platform?
    - Is access segmented or limited in any way to employees' job tasks?

But What About Centralized Cloud Data Storage? (cont.)

- **Ask these questions of contractors before agreeing to use centralized Cloud data storage for projects:**
  - Are subcontractors permitted access, and if so, is it read-only?
  - Does the contractor have the sole authority to backup data or remove it from the Project platform?
  - What is the contractor's Incident Response Plan?

Should You Pay a Ransomware Demand?



Should You Pay A Ransomware Demand? No.

- **Paying ransom may be illegal.**
- There is **no guarantee** that paying a ransom will prompt the release of the data
- **Do not engage the malicious actor.**

Should You Pay A Ransomware Demand? No. (cont.)

- Notify your insurance carrier if you have cyber insurance.
- Call a lawyer.
- Involve law enforcement.

Key Takeaway: Protect Yourself

Do not expect or rely on others to protect you

Negotiate full access to the project data file on the Cloud for your key employees, and regularly back up all data on the Cloud to your own network

PROTECTING YOUR PROJECT FINANCIALLY FROM DATA LOSS

Never Assume that Insurance Will Cover You

- **"Silent" Cyber coverage will soon be a thing of the past.**
- In response to the massive increase in malicious activity, general liability and property policy carriers are adding cyber incident or cybercrime **exclusions** to standard policies
- Do not assume that crime coverage will apply to ransomware attacks.
- Talk to your broker about the right cyber coverage for your project.

Negotiate Data Protection Into Your Contracts

- Require purchase of cyber insurance on the project as a matter of course
- Establish comprehensive guidelines for access to project data, backup of data, and disposal of data once the project ends, for all contractors, subcontractors and anyone else who will have access to data and make sure they are implemented
- Alert bidders about cybersecurity requirements at bid submission

Negotiate Data Protection Into Your Contracts (cont.)

- **Include comprehensive indemnification provisions**

- At a minimum, contractor must indemnify your company for all losses arising directly or indirectly from data loss, theft or inaccessibility - not just "data breaches"

- Write indemnification provisions clearly and broadly to include indemnification for cyber-crimes including ransomware or extortion, and for all consequences flowing from those crimes

Questions

Philip R. Stein
305-350-7220
pstein@bilzin.com

bilzin.com

bilzinlaw bilzinlaw bilzinlaw bilzinlaw