Nuts and Bolts Session

RDOS Cyber Attack
and other
Bits & Bytes

Presented by Danny Francisco

RDOS 2020 Rollercoaster

- March 2020
  - Covid Restrictions, New IS Manager
  - Remote work onboarding
  - Board/Corporation video meetings
- August 2020
  - Cyber attack
  - Christy Mountain Wildfire – EOC- Evacuations
- December 2020
  - RDOS IT Assessment Report to Board

Cyber Attack Wakeup Call

Good Monday Morning…or so we thought

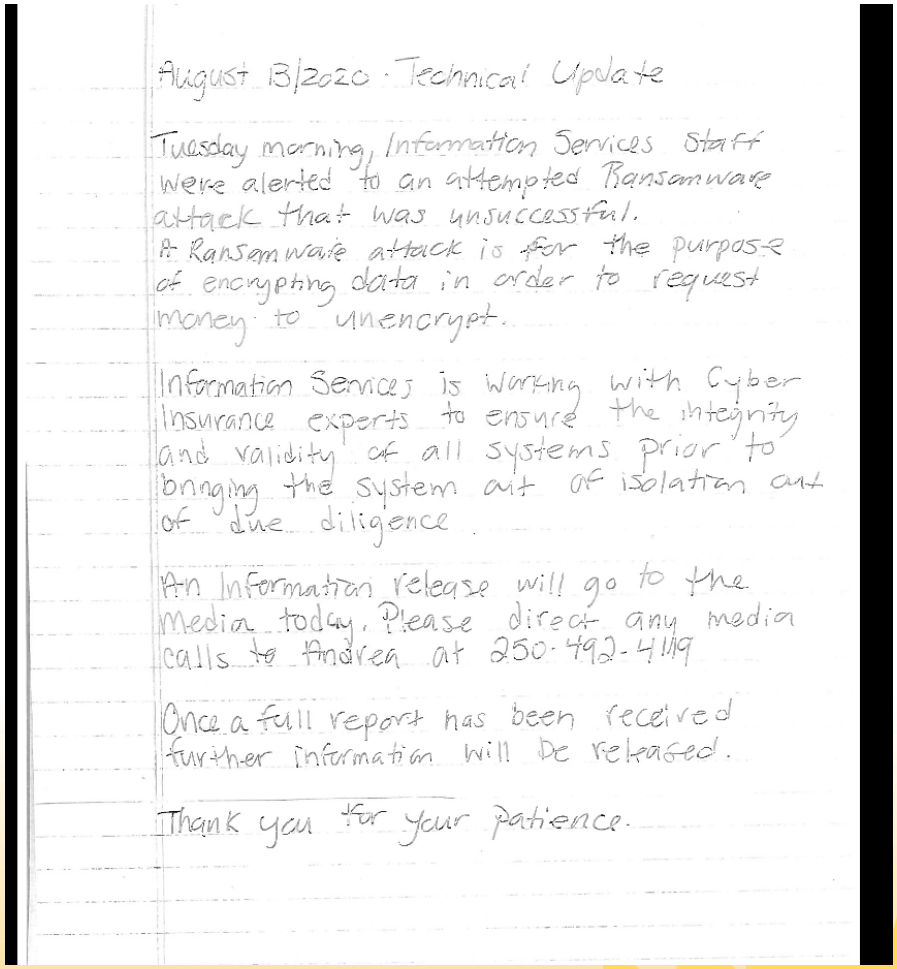
Cyber Attack….*&^%

First Day

- Affected systems
  - 35% Workstations, 95% Virtual Servers, 90% Onsite Backup Storage, VPN Connected remote sites
  - On site local Information systems that were Offline
    - File Shares/Document management, Email, GIS, Remote SCADA Access etc.

- Not Affected
  - VoIP phones, Network Firewalls and Switching infrastructure
  - Could Systems and non-VPN Connected remote sites
    - Public Website, Civic Ready, Employee Timesheet Tracking, etc.

Communication in 2020?



August 13/2020 - Technical Update

Tuesday morning, Information Services Staff were alerted to an attempted Ransomware attack that was unsuccessful.
A Ransomware attack is for the purpose of encrypting data in order to request money to unencrypt.

Information Services is working with Cyber Insurance experts to ensure the integrity and validity of all systems prior to bringing the system out of isolation out of due diligence

An Information release will go to the media today. Please direct any media calls to Andrea at 250-492-4119

Once a full report has been received further information will be released.

Thank you for your patience.

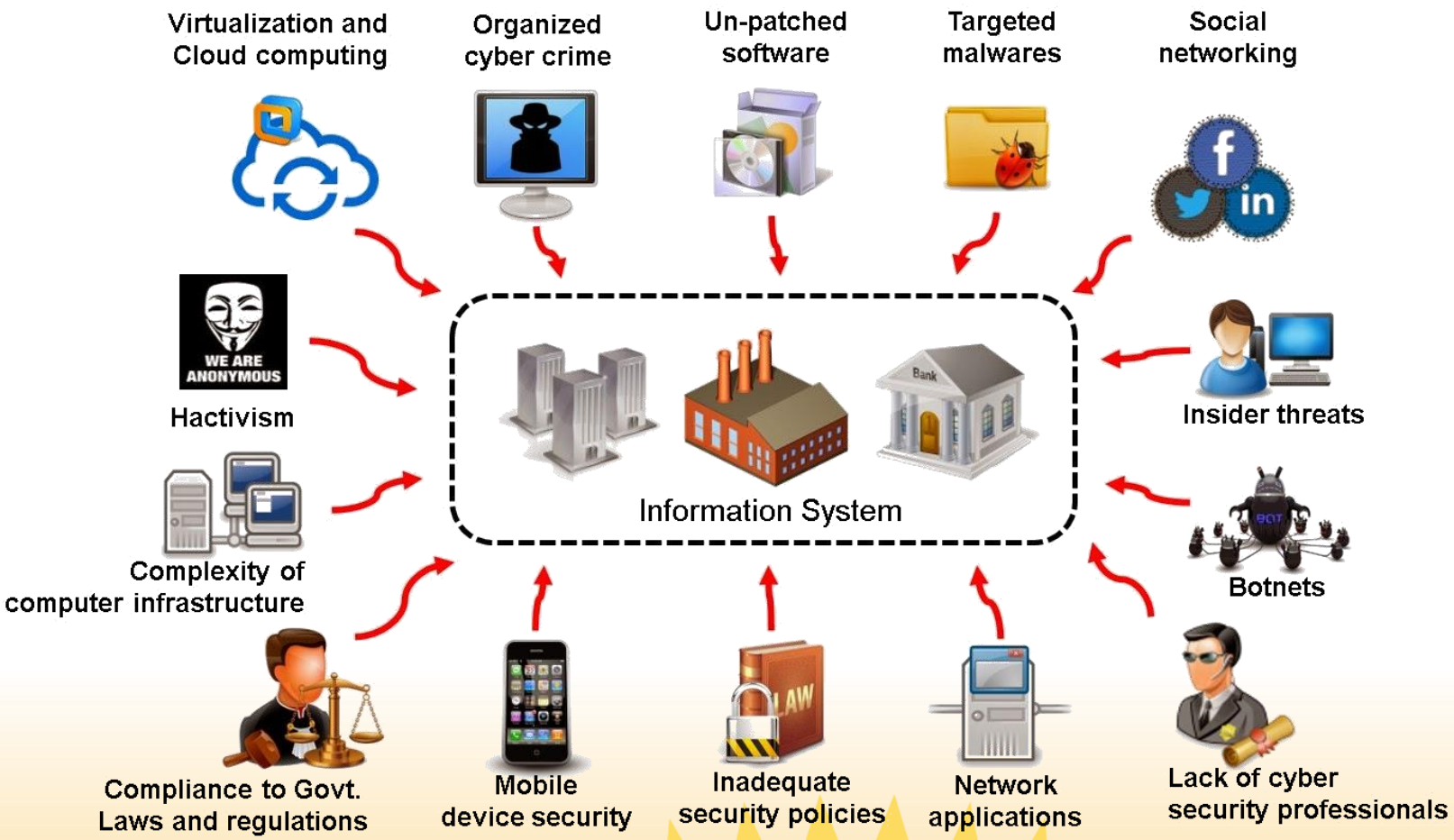
- ✓Paper Comm Letters
- ✓Handwritten Paychecks
- ✓"Sneaker Networks"
- ✓Paper Policy Binders

Cyber Attack…Now What?

First Week

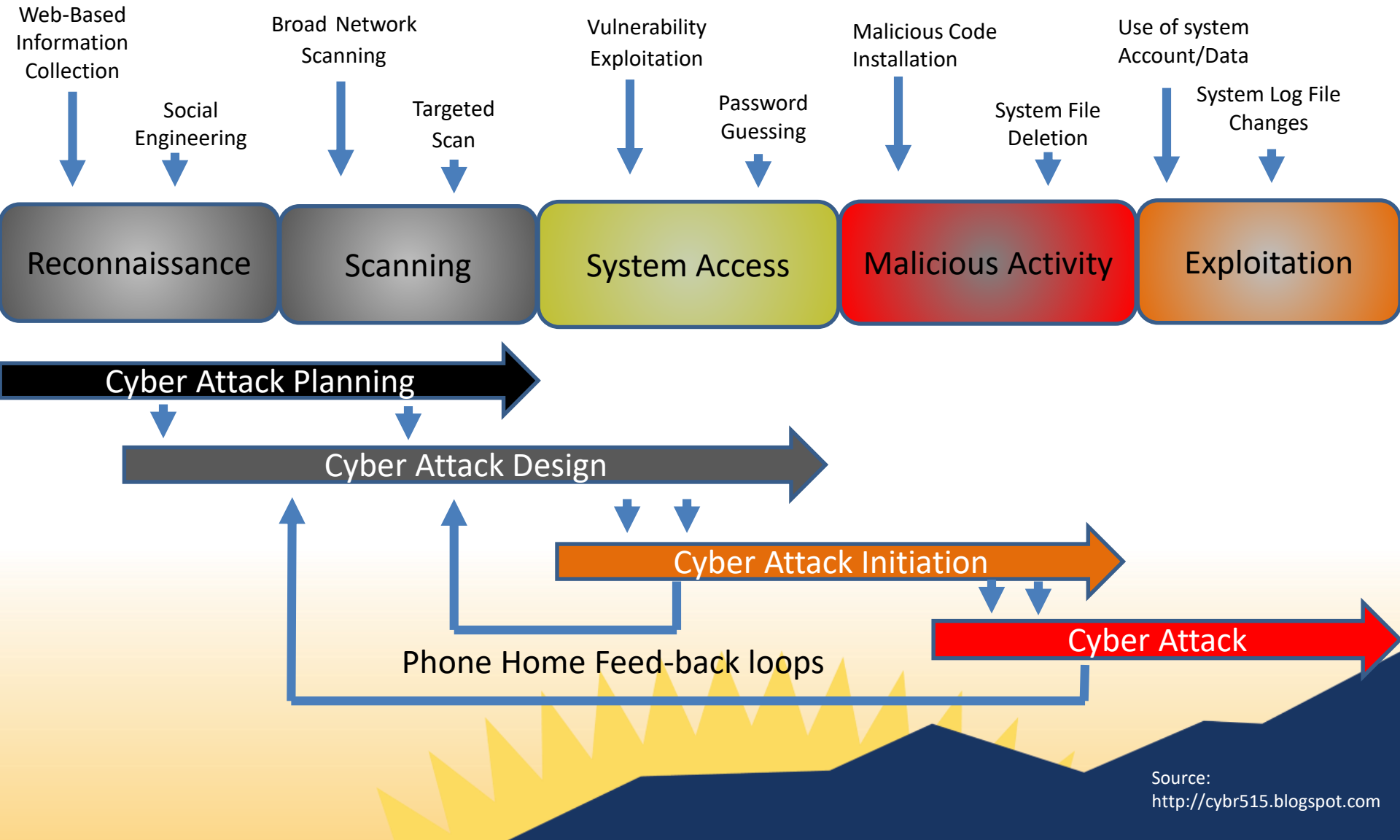
- Cyber Insurance Engagement
- Business Continuity Plan
- Disaster Recovery plan
- People Factor

How did I get attacked?



Source:
www.threatvectorsecurity.com

Cyber Attack Process



Source:
http://cybr515.blogspot.com

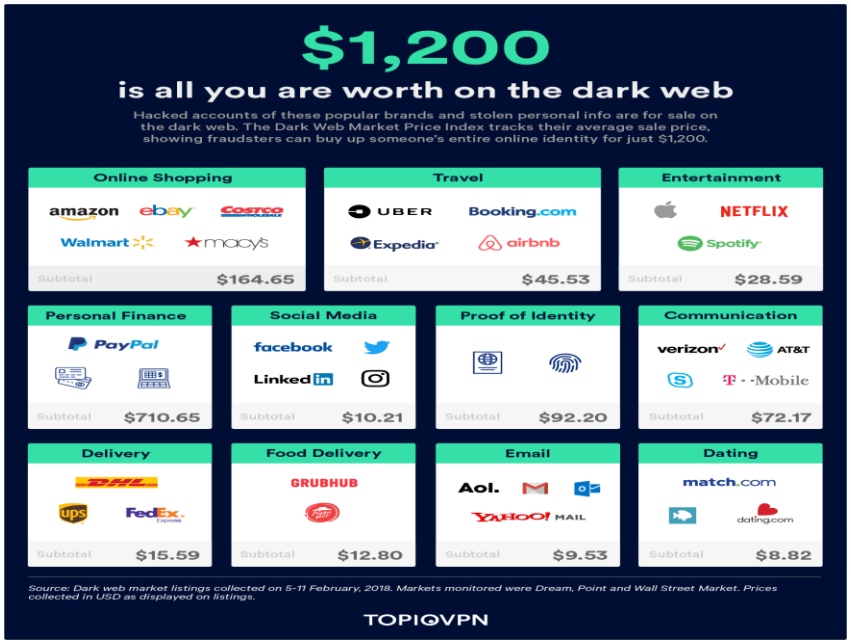
Cyber Attack...In a Nutshell

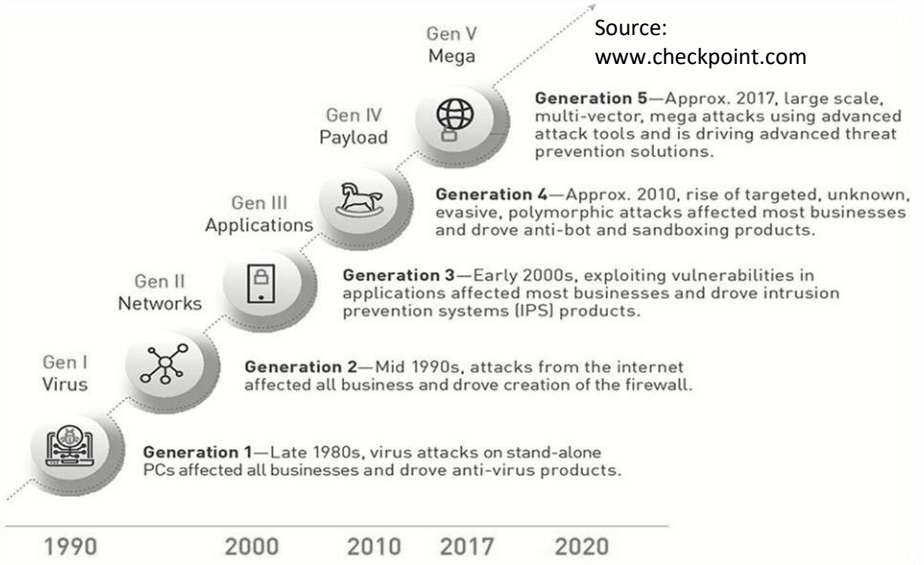
- Type of Attack?
  - Beta Ransomware *(PowerShell based)*
- From?
  - European Origin.
- Input Vector?
  - Compromised Account.
- Ransome Paid?
  - No, as attackers failed to fully execute.
- Recovery Time?
  - 5 Months

But we had Protection?

- Firewalls
- Password Policy
- Ransome ware Software
- Encrypted Hard drives
- Antivirus Software
- 2FA – Two Factor Authentication

Cyber World and Dark Web…





RDOS…next Steps?

- IT Assessment

  Completed in 2020 and implementing Recommendations

  - Rebuild core IT datacenter & infrastructure
  - Implement Enhanced Security Practices *(Identity Management, IT Processes)*
  - Implement server failover capabilities and improve Disaster and Business continuity plans
- Cyber Testing
  - Internal and External Penetration Testing, 3rd Party Network Audits
- Education and Safety
  - Cyber Security all staff responsibility, not just IT.
  - Phishing and Cyber safety education
- Utility Thinking
  - IT has become a “Utility Service”
- Regional Thinking
  - Collaboration
  - Cost and Resource Sharing

Thank You

Contact Info:

Danny Francisco • Manager of Information Services
Regional District of Okanagan-Similkameen
101 Martin Street, Penticton, BC V2A 5J9
p. 250.490.4127 • tf. 1.877.610.3737 • f. 250.492.0063
www.rdos.bc.ca • dfrancisco@rdos.bc.ca
FACEBOOK • YOUTUBE • Sign up for REGIONAL CONNECTIONS