Welcome to Our Journey... So Far

Presented by: Ken Shannon
Manager, IT Infrastructure & Security
Haas Automation Inc.

HAAS

Haas F1 Team
OFFICIAL MACHINE TOOL

Agenda

- Over 100 slides of action-packed material
- Educational videos
- Interactive sessions
- Blah, blah, blah
- Just kidding…

KEEP
CALM
AND
NO
AGENDA

Quick history of Haas Automation Inc.

- 1975 - **Gene Haas** worked in machine shops after graduating college
- 1978 – Opened a small machine shop called Pro-turn Engineering
- 1983 - **The founding** of Haas Automation Inc. (in Sun Valley, CA)
    - the first fully automatic, programmable collet indexer
    - expanded product line to include fully programmable rotary tables, rotary indexers, and machine tool accessories
- 1988 - **The debut** of the first Haas CNC machining center (the VF-1) at IMTS.
        - (You can see the very first VF-1 outside in the Demo Room)
- 1991 – **Move** to larger facility in Chatsworth, CA
- 1997 – **Move** to purpose-built facility on 86 acres in Oxnard, CA
- 2005 - The building, sales and shipment of **10,000 machine tools in one year**, a record increase of more than 22% over 2004 and more than 200% over 2003.
- 2018 – Shipment of **15,960 machine tools in one year** – a record year.
    - Now a total of over 200,000 machines produced in our history.

Quick history of Haas Automation Inc. (cont'd)

- Fast facts:
  - Currently about 1,500 employees worldwide PLUS ~300 temps
  - Here in Ventura County includes:
    - Head Office / Manufacturing facility (Oxnard)
    - Haas Sheet Metal Fabrication facility (Oxnard)
    - Warehouse (Camarillo)
  - Haas Europe – Brussels, Belgium
  - Haas Asia – Shanghai, China
  - TBD - Henderson, Nevada (announced last week)

Even quicker history of Haas IT (as I remember it)

- Prior to 2007 - ???
- Haas implemented SAP in July, 2007
- I started in August, 2007 as an SAP System Administrator
  - Joining a "Helpdesk" team of 6 staff that did EVERYTHING
- Promoted to IT Manager in 2011
- About 4 years ago, we start increasing awareness of Cyber threats – particularly due to what we heard in the news

So our journey begins

- We've always had firewalls and AntiVirus!
- As we hear of Ransomware, Bitcoin and others on the rise, we start to prepare ourselves:
  - Read articles
  - Listen to podcasts
  - Attend webinars and seminars
  - Start to lose sleep…

The first steps and challenges

- Removal of local administrator rights
  - A huge end-user cultural change (not always the “HAAS way”)
  - Issues with legacy or specialized software applications
  - IT HelpDesk staff:
    - Needed to “accept” this on their own systems
    - Learn to support end-users with this new “twist” – many remotely
- Replacing of systems with out-dated Operating Systems
  - Many systems still had Windows XP and MS Office 2003 (enough said!)
  - Servers were old too – Windows Server 2000 and 2003

The first steps and challenges (cont’d)

- Regular scheduling of O/S and application patching
  - Seemed more challenging that it needed to be
    - Users didn’t like their systems restarted automatically
    - AND didn’t like to restart regularly either
    - SO patches installed but not taking affect until restart!
- Simulated Phishing testing and training
  - Initial “click rate” results were recorded at 10-12%
  - Training was considered “non-productive” so seldom completed
  - Repeated testing and remedial training with mixed success

The first steps and challenges (cont’d)

- Attempts to stop “Shadow IT”
  - Other departments were purchasing hardware & software
    - Complete systems from vendors to operate machines
    - Apple MacBooks & iPads on credit cards
    - Miscellaneous software (including Salesforce)
  - Once in the door, we have to support it!

Small wins and successes

- After the General Manager received a call directly from a vendor that we didn't know we had purchased software from, I explained the problem with Shadow IT and he soon announced that ALL IT-related purchases MUST go through IT.

- A number of employees have personally thanked us for either the online or in-person Cybersecurity training
  - Helped them or loved ones recognize suspicious phishing attempt

Haas F1 Team
OFFICIAL MACHINE TOOL

And some potholes too.

- Numerous attempts and near-misses – including (but not limited to the following):
  - Numerous CEO Fraud and spearphising email attempts
  - One external-facing server contained malicious code to re-direct users
  - Two external-facing servers with “Coin mining” found
  - Two Haas dealers hit with Ransomware
    - One down for 3 days, the other down for 1 month
  - One Haas dealer website hacked and pornographic website embedded

GDPR?

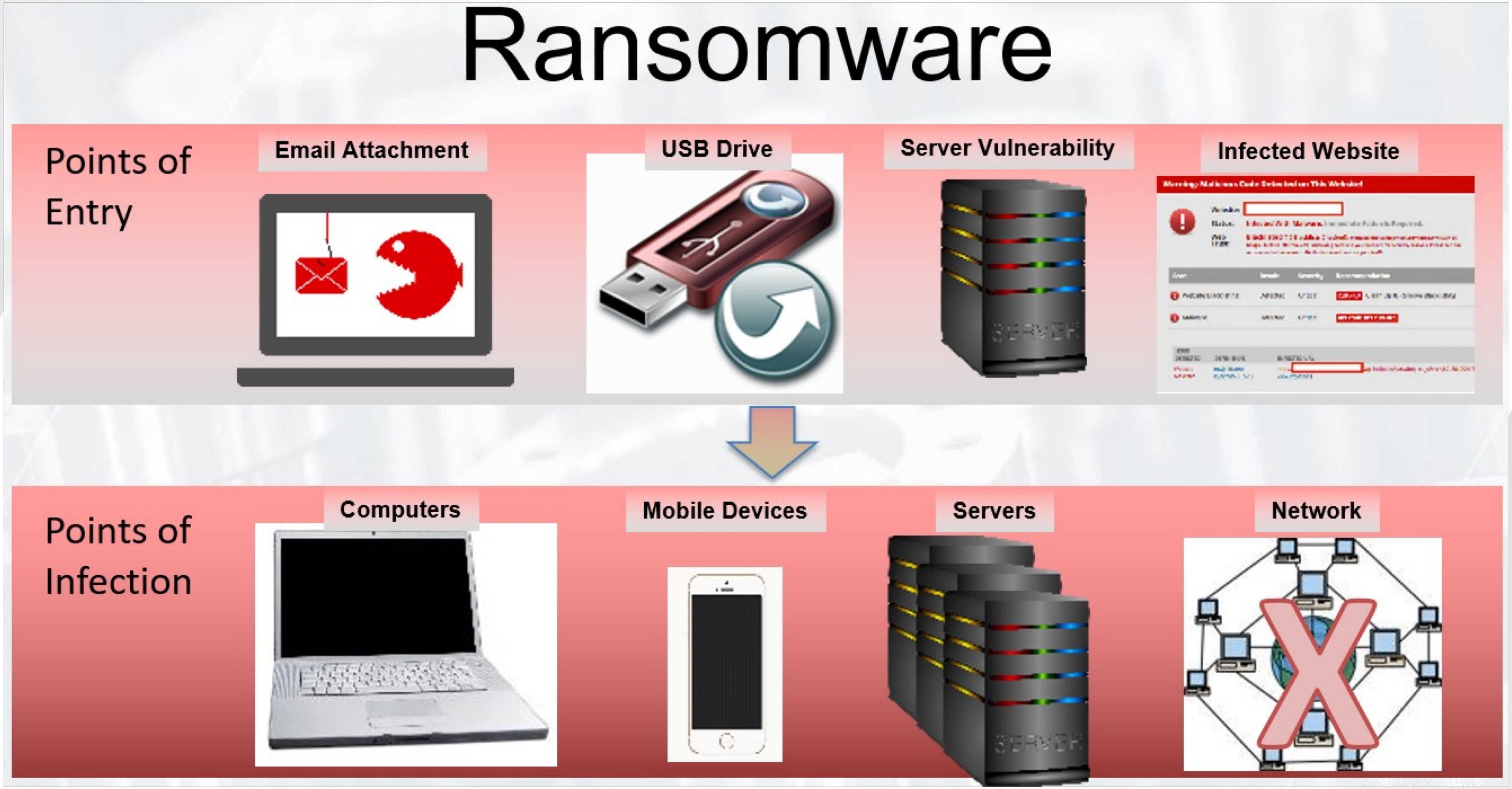
- European Union’s General Data Protection Regulation
- Effective May 25, 2018
- Protects privacy of EU citizens
- Affects any company with EU employees, customers or vendors
- Followed by:
  - China’s Cybersecurity Law
  - Privacy Laws & Breach Reporting by all (or most) US states

GDPR? (cont’d)

- Conduct a GDPR “Readiness” Assessment
- Conduct an “Information Security Program Posture Assessment”
- Honestly, both of the above were NOT great results due to:
  - Lack of policies
  - Minimal written procedures
  - No “Privacy by Design”
  - Little to no encryption
  - No formalized Information Security Program

Why is all this important?

- Presentation given to Executives on Information Security and GDPR
- Listed recent attacks and issues encountered to-date
- Explained why Information Security is important to help us continue to build machines and stay in business
- Used the following 2 slides (my favorites):



Ransomware

Points of Entry

Email Attachment

USB Drive

Server Vulnerability

Infected Website

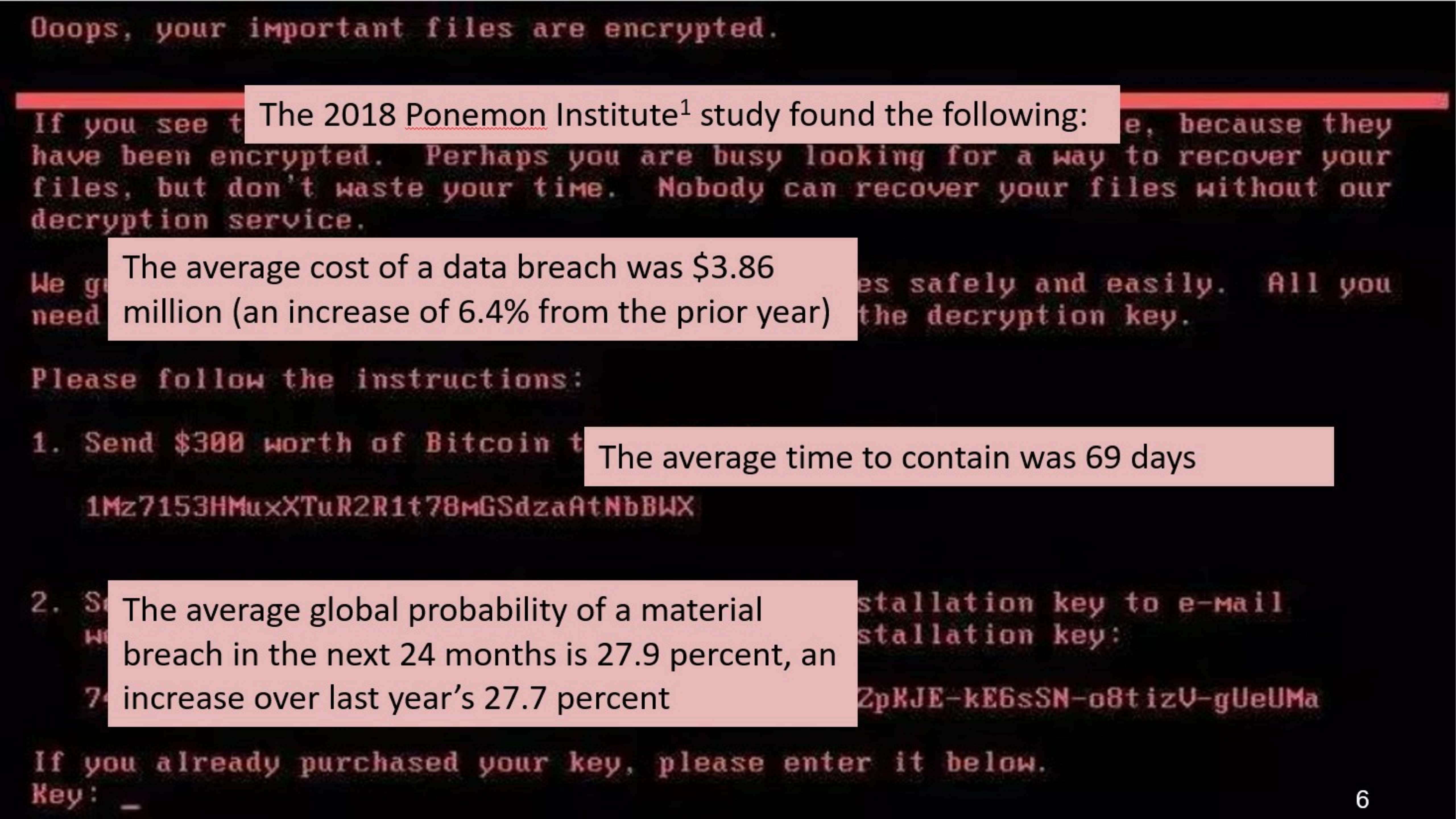
Points of Infection

Computers

Mobile Devices

Servers

Network



```
Ooops, your important files are encrypted.

If you see t                                                    e, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We g                                           es safely and easily.  All you
need                                           the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin t

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. S                                           stallation key to e-mail
   w                                           stallation key:

   7                                           ZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```

The 2018 Ponemon Institute[1] study found the following:

The average cost of a data breach was $3.86 million (an increase of 6.4% from the prior year)

The average time to contain was 69 days

The average global probability of a material breach in the next 24 months is 27.9 percent, an increase over last year's 27.7 percent

Why is all this important? (cont'd)

- Executive level support for resources and funding
  - Communicated to staff at all locations.
- Started the GDPR & Information Security program roadmaps
  - Using ISO 27001
- Created an Enterprise Security team (Kyle & Zane)
- Purchased software
  - Vulnerability Scanning
  - SIEM

Next steps

- Data Classification & Data Retention
- Encryption and Data Protection Program
- Data Loss Prevention (DLP)
- Data Breach Response Plan
- Risk Management Program
- Vendor/Supplier Governance Program
- And the list goes on…

Still a long road ahead of us…

Questions?

Haas F1 Team OFFICIAL MACHINE TOOL