PONDURANCE

Cyber Security Risk

Be Secure While Managing Tech Enabled Growth

Ron Pelletier | CISSP, CBCP, CISA
Founder

AGENDA

A Look at Tech Risk

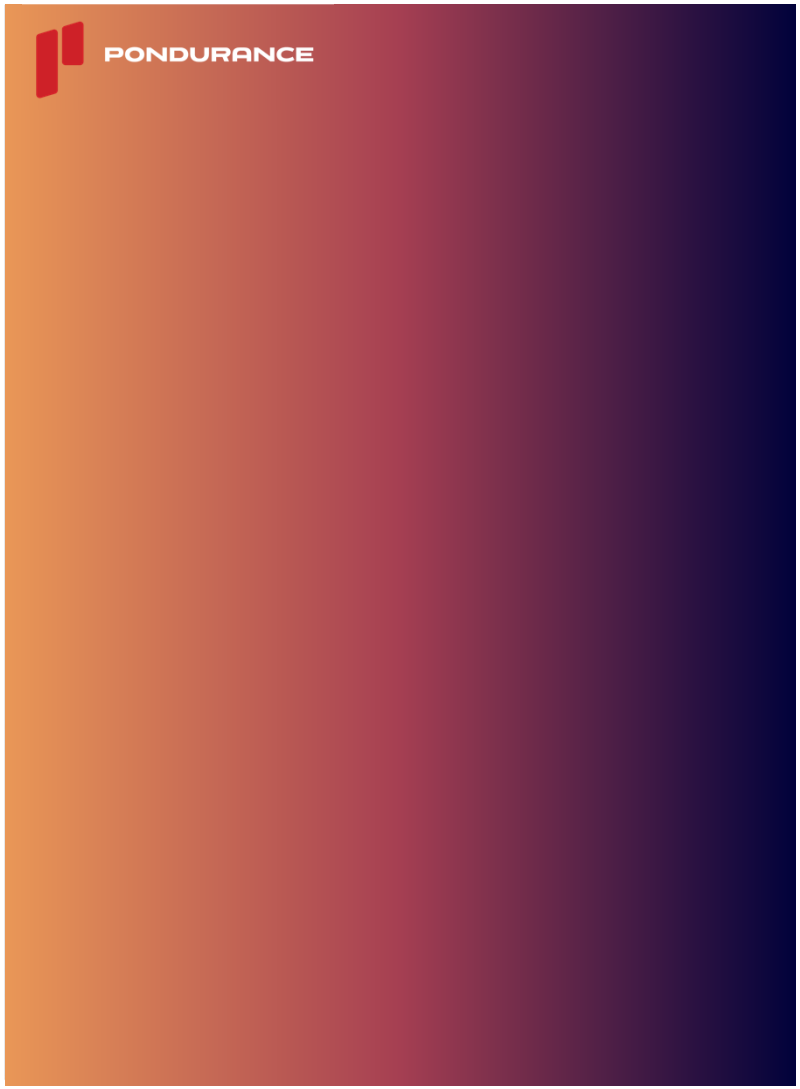
Feasibility of Breach Prevention

QUESTIONS

Tech Enabled Growth is Inescapable…is the Breach Inevitable?

- What is your risk on the availability of electronic records?
- Does collective storage increase or decrease risk to data?
- What role will the cloud play in your system and data integration plans?
- Can medical devices by hacked and do regulatory requirements extend to the patient end point?
- Are mobile devices at greater risk because of their portability?
- How is output derived from input, and why should I trust a computer for a diagnosis?

What Motivates a Bad Actor?



- **Street Cred** – Proving they can do it for their own ego
- **Hactivism/Denial of Service** – Keeping you from operating
- **Steal & Use Your Data** – Corporate espionage is alive and well
- **Steal & Sell Your Data** - Identities/cards are sold on the dark web
- **Steal Your CPUs & Bandwidth** – Cryptojacking is becoming more and more of a problem
- **Steal Your Money** – Tricking someone into giving it up
- **Hold Your Data Hostage** – Ransomware has made big headlines and will continue to be a viable strategy for bad actors

Mitigate Intolerable Risk

IS BREACH PREVENTION AN IMPOSSIBLE ENDEAVOR?

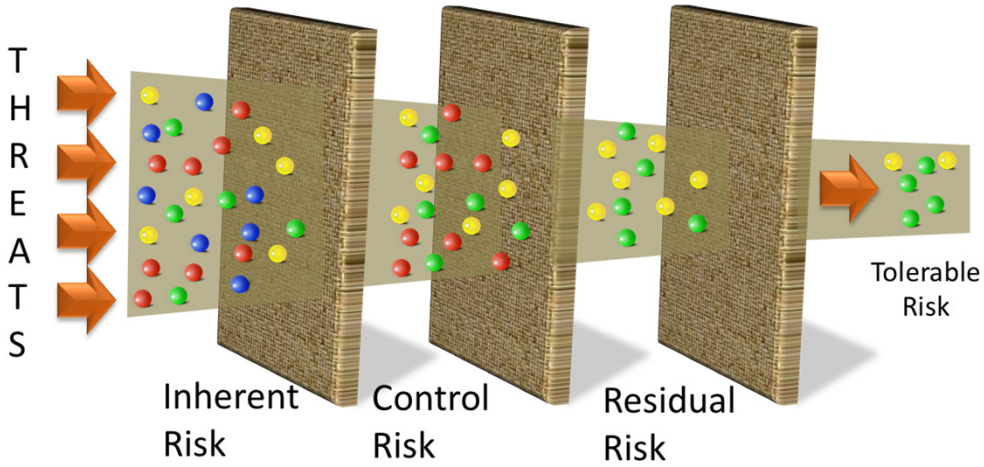
You don't always have to out-run the BEAR…

» Define Your Risk Tolerance

- You may not have to spend $1M on security
- Know your threat landscape
  - What do I have?
  - Who would want it?
  - How would they get it?
  - What is the likelihood and impact?

» You CANNOT Prevent Every Breach

- Sometimes, just being good enough is ok
- But you can and SHOULD reduce the likelihood of occurrence
- Lessen the risk to tech enablement
  - Vulnerability Management
  - Multi-Factor Authentication
  - Next-Generation Anti Virus
  - Active Threat Hunting (Tech + People)
  - User Awareness Training



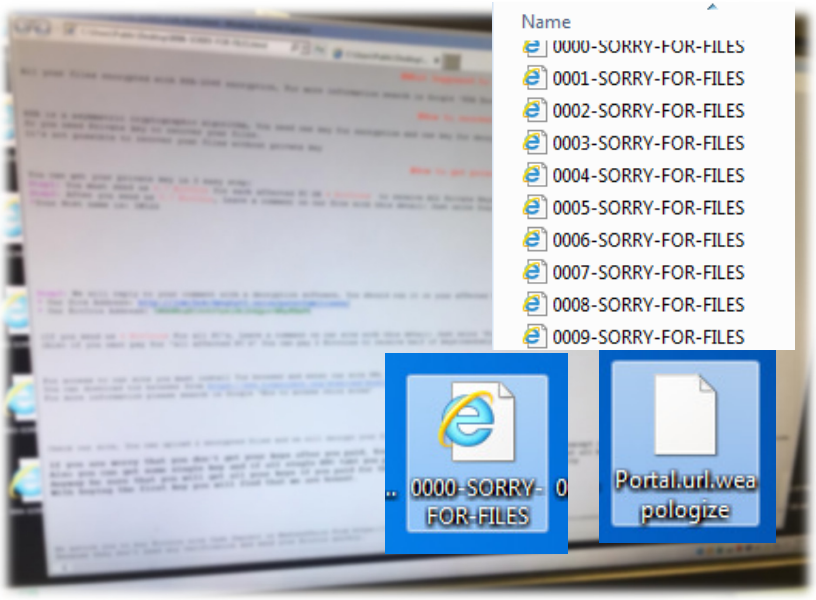
How Can I Extend My Security Controls to my Extended Tech?

- Develop robust continuity and availability plans for your tech and your data…you may need it sooner than you think
- The cloud can be a safe haven for data if you make it so…but leave it to chance
- Enable robust encryption where possible to mobile devices and data in transit
- Ensure clean, verified, and accessible backup data is at hand…and the restoration is tested
- KNOW the security posture of your vendors

...But what if the breach DOES happen?

1. Availability
   - Requires complete dedication to the task at hand. Lead from the front
2. Selflessness
   - It's not about you, it is about getting it right. No egos allowed.
3. Decisiveness
   - Don't second guess yourself. Use the data, make a plan, and stick to it
4. Flexibility
   - Don't confuse decisiveness with inflexibility. New information may prompt a change
5. Delegation
   - Trust your team. You can't do it by yourself.
6. Honesty
   - Truth is integral to this process. If it happened, own it

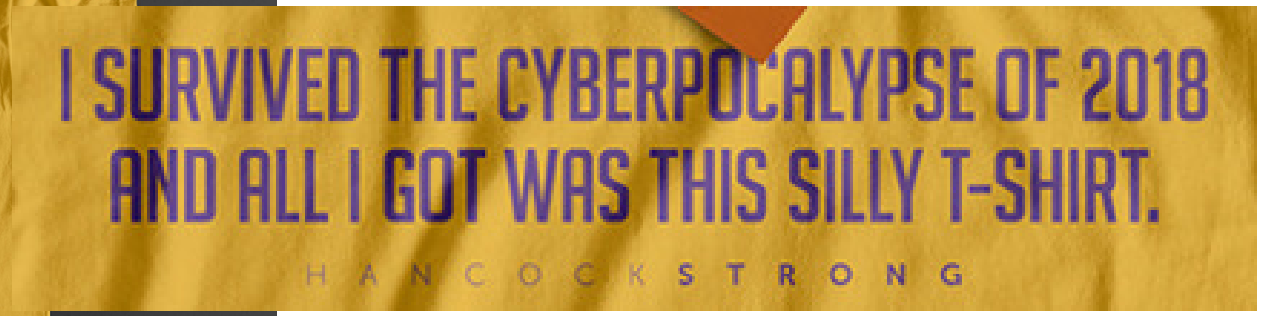
2018 Hancock Health Ransomware Event



- Jan 11, between 9:30 – 11:00 p.m., SamSam ransomware event renders production systems and data unusable
- By 1 p.m. on Jan 12, CEO Steve Long made the decision to pay the ransom (4 bitcoin, roughly $55k)
- **Steve was calm, decisive and entirely transparent in all regards**
- Communication flowed regularly, status meetings every 2 hours
- By Jan 14, critical systems operational
- Results of forensics examination may mean no data breach…**LOGGING WAS CRITICAL!**

In the Aftermath, They Celebrated!

HancockHealth



Strength *noun*

1 : the quality or state of being strong
2 : power to resist force | solidity, toughness
3 : power of resisting attack
4 : the ability to deal with difficult situations

The strength of Hancock Health is measured by our team of associates, doctors and volunteers. Our team is strengthened with the love and support of family and friends.

HANCOCK**STRONG**

Consider These Action Items Your Critical Path

1. Confirm the scope of the incident
2. Activate Incident Response Plan
3. Contact key parties (legal counsel, IT forensics, FBI)
4. Initiate downtime procedures
5. Confirm all information before communicating
6. Communicate upward AND downward
7. **Contain and eliminate the threat, move to recovery**
8. Stay calm, foster strong leadership

QUESTIONS?


THANK
YOU
PONDURANCE
SECURITY. CONTINUITY. COMPLIANCE.