# Cybersecurity Steps Every Healthcare Organization Should Take Now

Corey White | CEO & Co-Founder
Craig Goodwin | COO & Co-Founder

CYVATAR.AI

The Future Of Cybersecurity

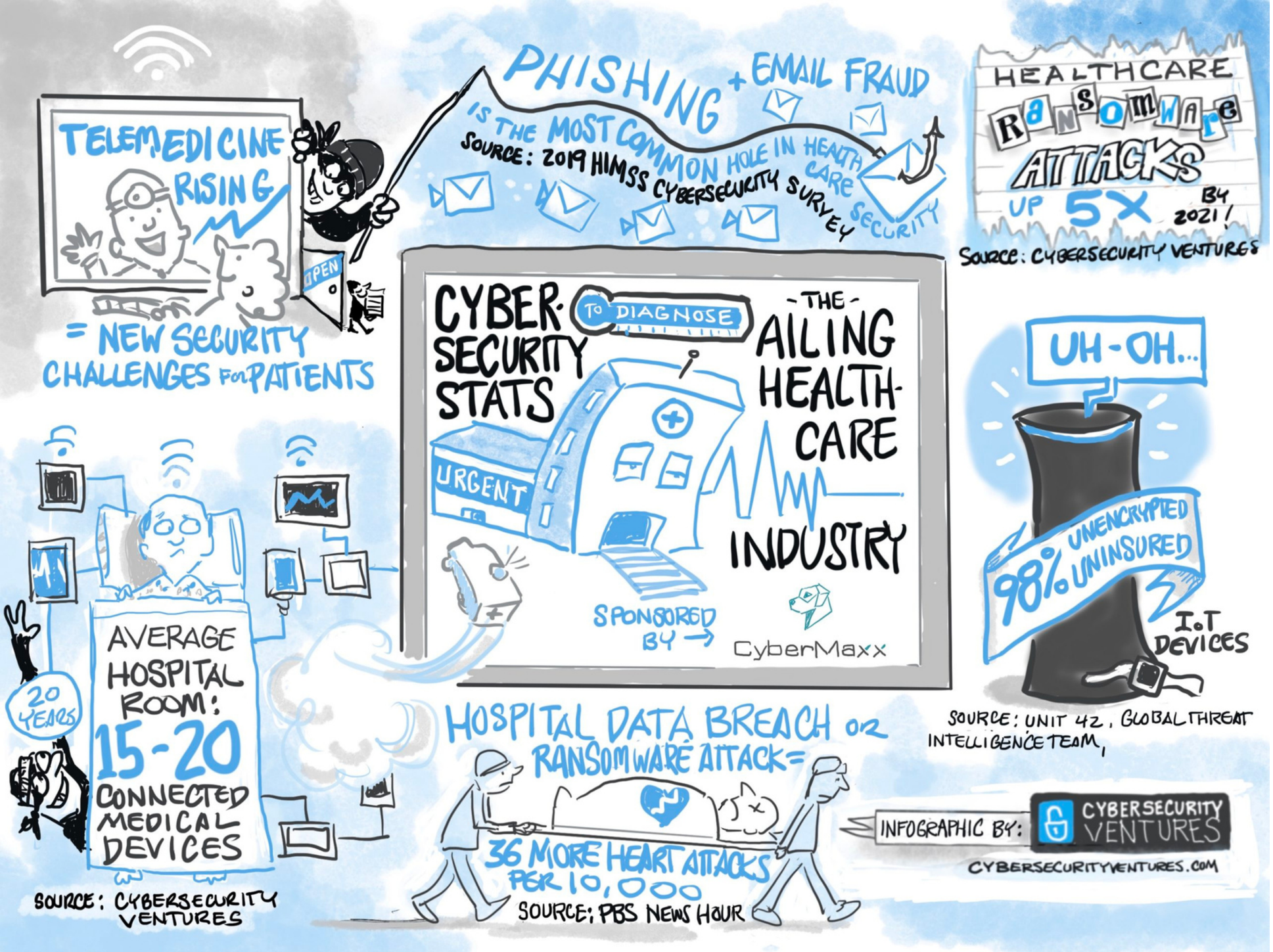
# About Corey + Craig

**Corey White**
*CEO & Co-Founder*

- Over 25 yrs information security experience
- Former SVP of Worldwide Consulting & Chief Experience Officer of Cylance
- Managed team of 200 consultants
- Developed first Compromise Assessment
- Developed ThreatZERO – first outcome based security solution
- Former Director of Consulting for Foundstone & McAfee/Intel Professional Services

**Craig Goodwin**
*COO & Co-Founder*

- Over 20 yrs CISO / CSO Experience
- Former Chief Trust & Risk Officer at Fujitsu
- Global CISO for a number of large PLCs including Ferguson Group, Monster Worldwide & CDK Global
- Customer Advisory Board member for Splunk, National Cyber Security Alliance (NCSA) & YL Ventures
- Built and lead global product and security portfolio offerings for a number of large technology businesses




Healthcare continues to be a key target for Cyber Attacks as well as the culprit for many data breaches, this is expected to rise in to 2023 and beyond.

# Breach Data | Network & Email Security

There have been 508 HIPAA breaches reported so far in 2020. In total, 22.3 million Americans have had their PHI compromised

“68% were reported as hacker / IT incidents, representing 91% of the total individuals affected by all breaches.”

The maximum penalty for a single breach is $1.5 million per year. For one violation, fines can range from $100-$50,000 for each instance of wrongdoing.

But...They likely all originated on an endpoint.

# Compliance v. Security

## Unfortunately, you need both...

# Buy Some Tools!

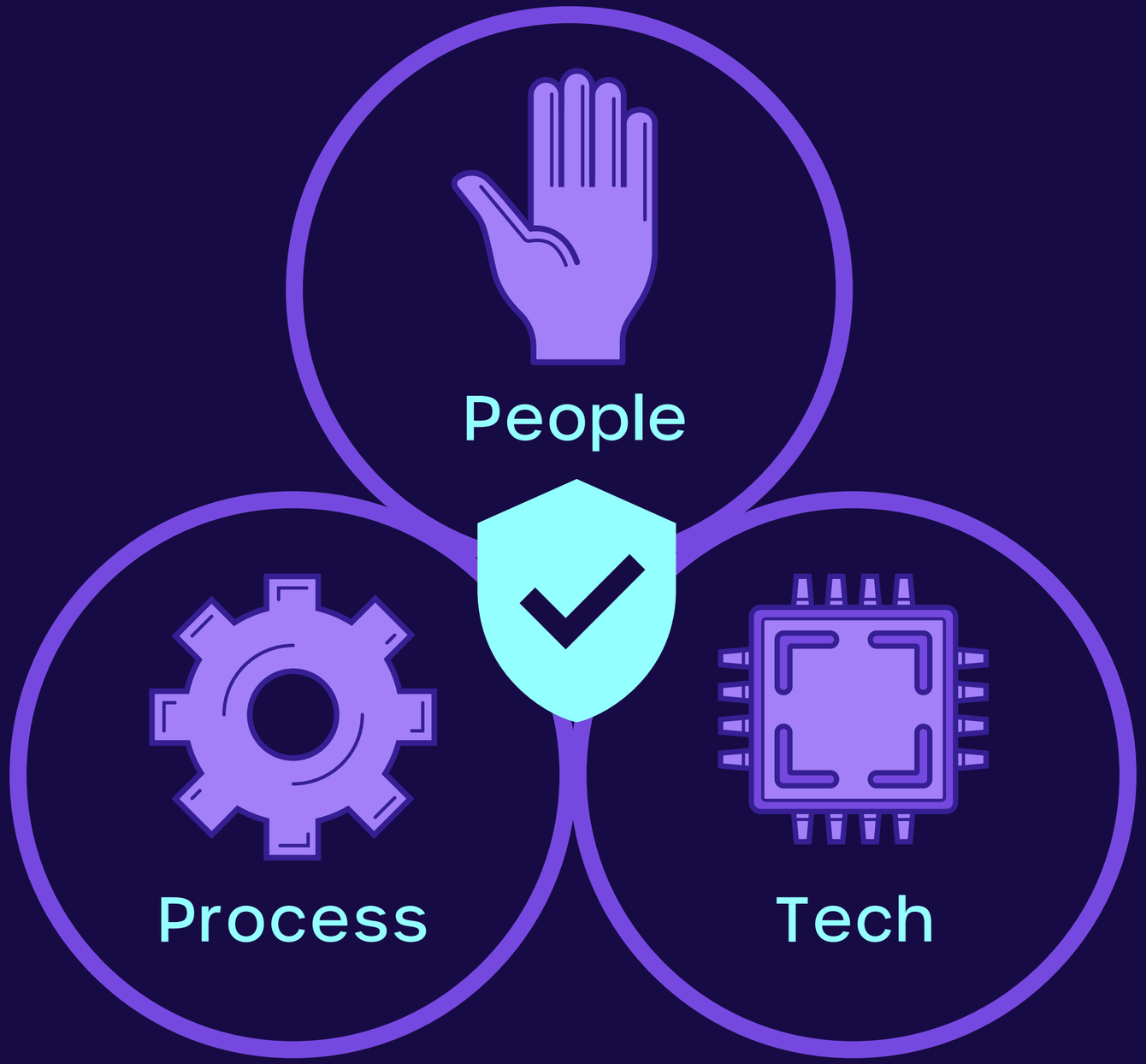
TOYS

# Buy Some ~~Tools~~!

It’s much more than just the technology

# The Security Triad

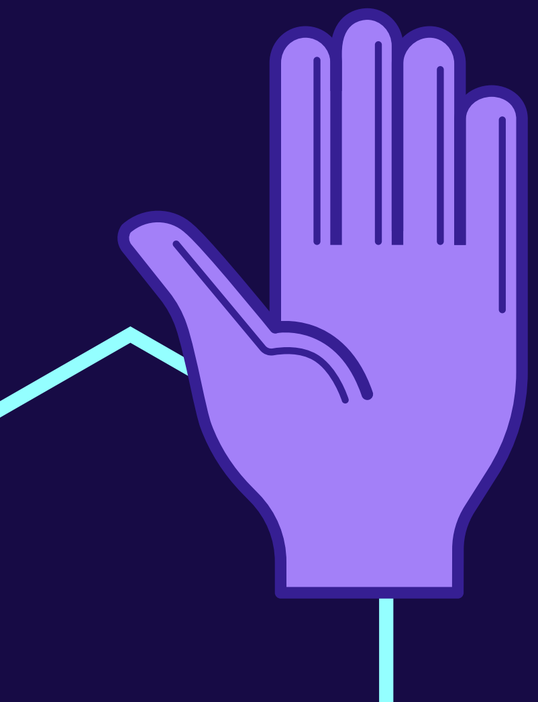
Organizations must address all components to really make a difference



# People

# What's the Problem?

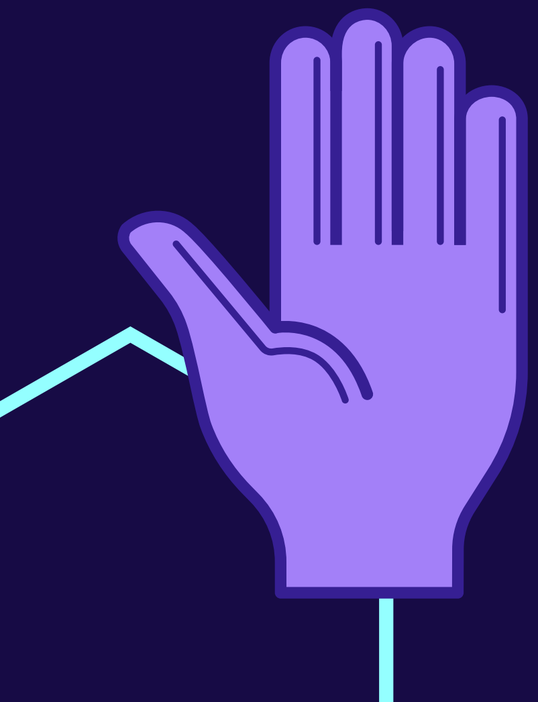
People are often the weakest link, but we shouldn't blame them



- People often provide the easiest route in to an organisation
- Human error is normally the biggest cause of the initial breach
- Phishing emails and Business email compromise continue to rise
- We are not pre-conditioned to follow security rules
- We are more accustomed to the physical world

# Simple Steps?

Make people aware and give them the training



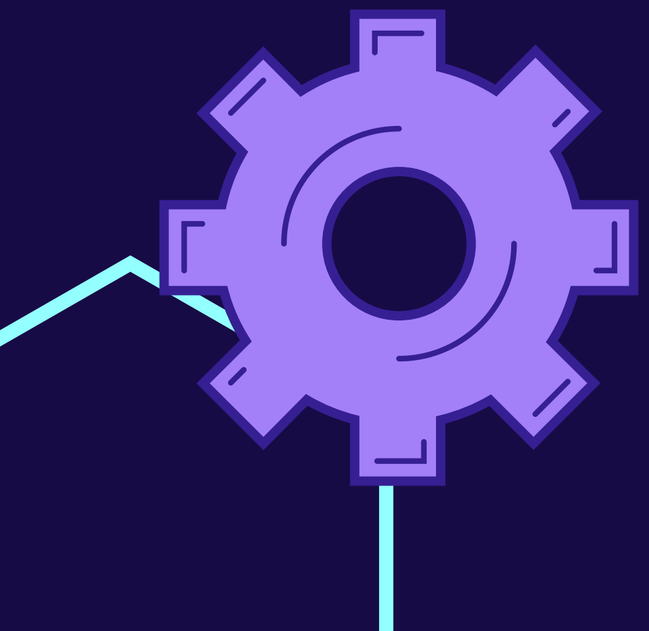
- Educate your people on what they should be looking out for
- Build a culture of speaking up and asking
- Extend advice to outside of work
- Consider social engineering
- Consider formal training for at least a member of staff
- Leverage your vendors where you can
- Grant access only on a ‘Need to’ basis


Process

# What‘s the Problem?

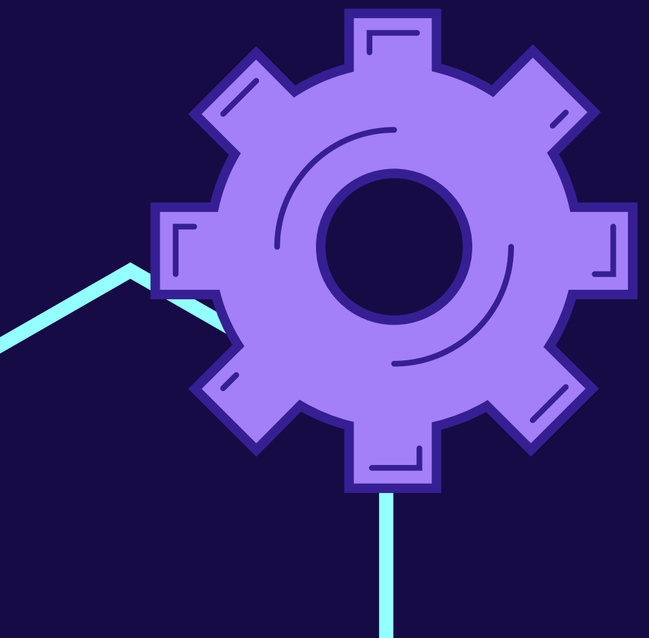
You need good process to stitch everything else together

- •Everything can not be solved by technology alone
- The ‘way‘ in which you do things is just as important
- Data Handling – Physical as well as Technical
- ‘How‘ you utilise technology and people
- Policies and Procedures outline the fundamentals
- Often it‘s a failure in process rather than technology that causes the issues

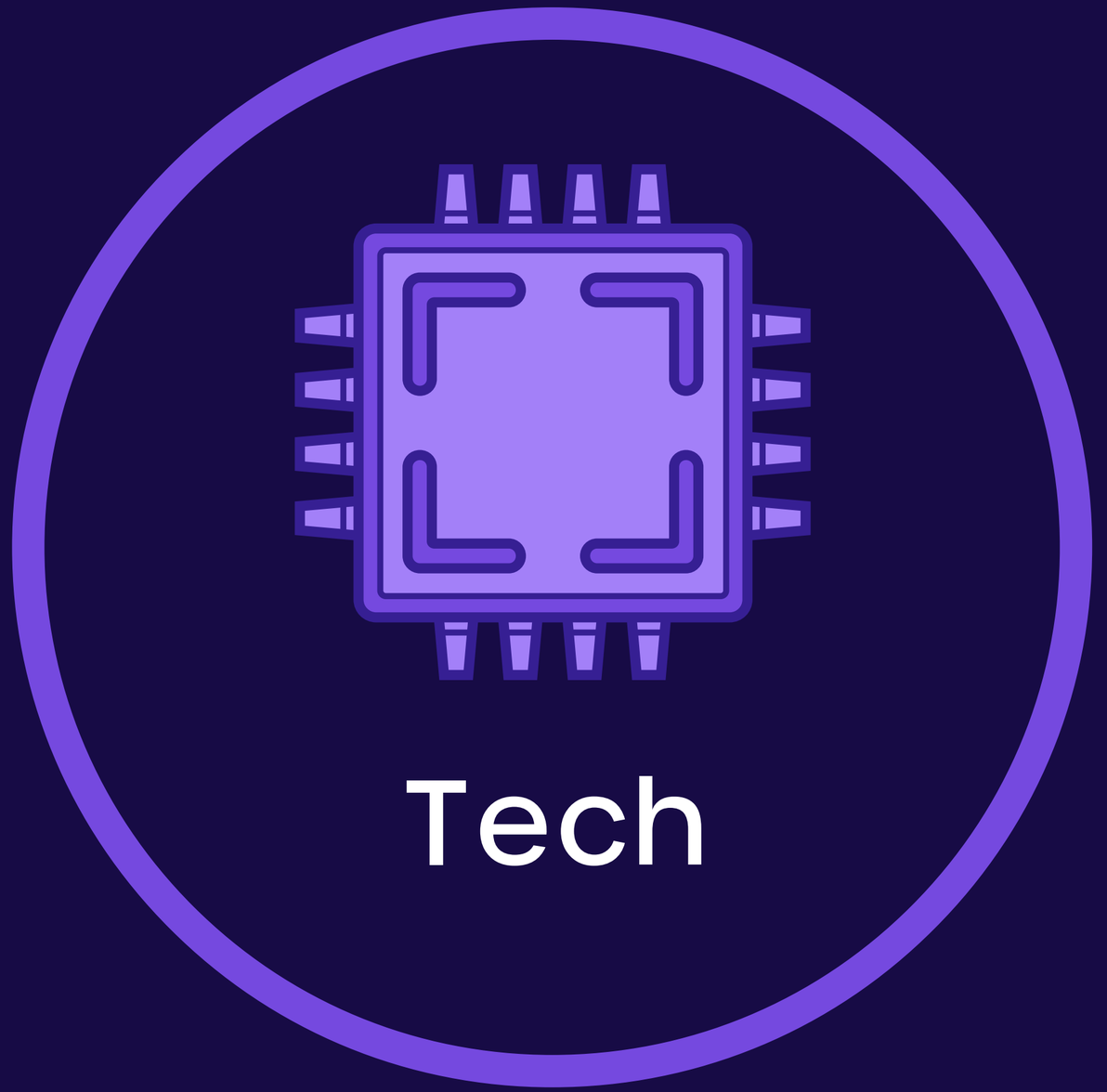


# Simple Steps?

Build basic processes and policies, then communicate them



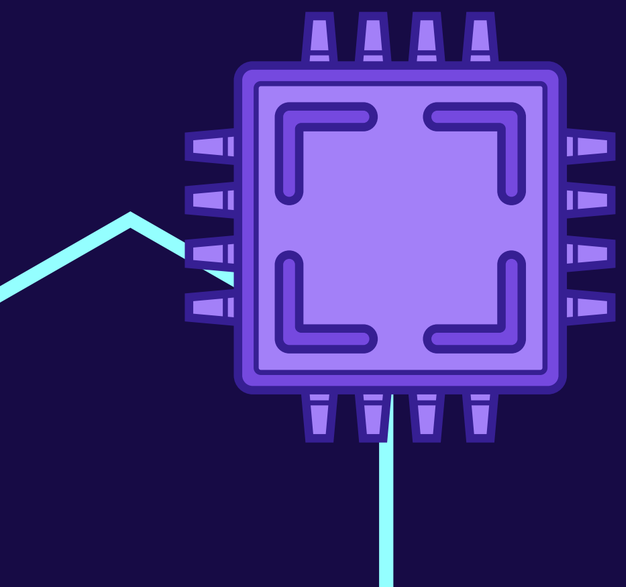
- Find the data, work out from there
- Build simple processes, don’t let great be the enemy of good
- Think about your supply chain, follow the data
- Over-communicate with all staff involved
- Utilise industry benchmarks and templates



# Tech

# What’s the Problem?

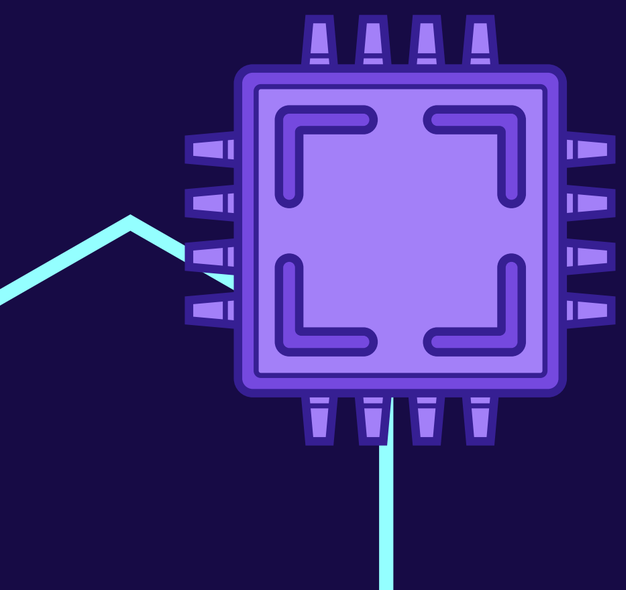
It’s very complicated and you need the basics



- Thousands of security tools on the market
- A lot of marketing Fear, Uncertainty and Doubt
- Everything is important, so its not always easy to know where to start
- Compliance standards drive you towards a ‘tick-box‘ approach
- Do not neglect the obvious, or the basics

# Simple Steps?

## Start with the Basics



- Start with the basics, even in larger organisations
- The majority of breaches occur on end user systems (Laptops and Desktops) so invest there
- Focus on the 80% for the most effective investments
- Focus on the people and processes to educate and upskill
- Building in process and policy can be cheap and effective

# What Should Every Healthcare Organization Be Doing Now?

- Start with the basics, even in larger organizations
- The majority of breachesoccur on end user systems (Laptops & Desktops) so invest there
- Focus on the 80% for the most effective investments
- Focus on the people and processes to educate and upskill
- Building in process and policy can be cheap and effective

# Thank you!

corey@cyvatar.ai
craig@cyvatar.ai

**Learn More at cyvatar.ai**

CYVATAR.AI

The Future Of Cybersecurity