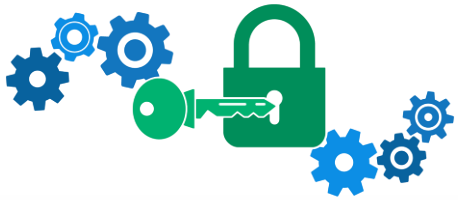
OPEN DOOR
FAMILY MEDICAL CENTERS

A Real Security Encounter
Cyber Terrorism!

Mikkel Finsen
Open Door Family Medical Center
Snr Director IT & Security Services
18 November 2020

About Open Door



Open Door Family Medical Centers
- est. 1972
- Fully Qualified Health Center
- HQ in Ossining, NY

- Approx. 500 employee
- 6 main sites in Westchester
- 10 school-based health centers
- 60000 patients

Medical, dental, and behavioral health care

Promote wellness, good nutrition, stress reduction, and physical activity.

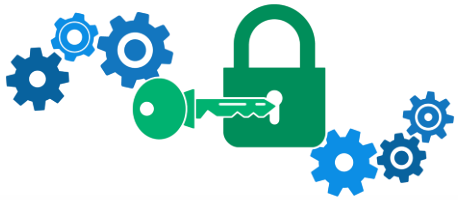
Mikkel Finsen

Joined in September 2019 as Head of IT, after 21 years with KPMG.

Transforming IT to enterprise level organization, supporting the growth and productivity.

1. Assess and improve the infrastructure, platforms, and processes
2. Enhance security tools and levels
3. Increase user awareness – developing a secure mindset
4. Work with internal stakeholders on gaining more efficiencies from applications

Our Security Level



Back-up Restore

Full back-up solution in place
Back up sent to cloud

Anti Virus & Firewalls

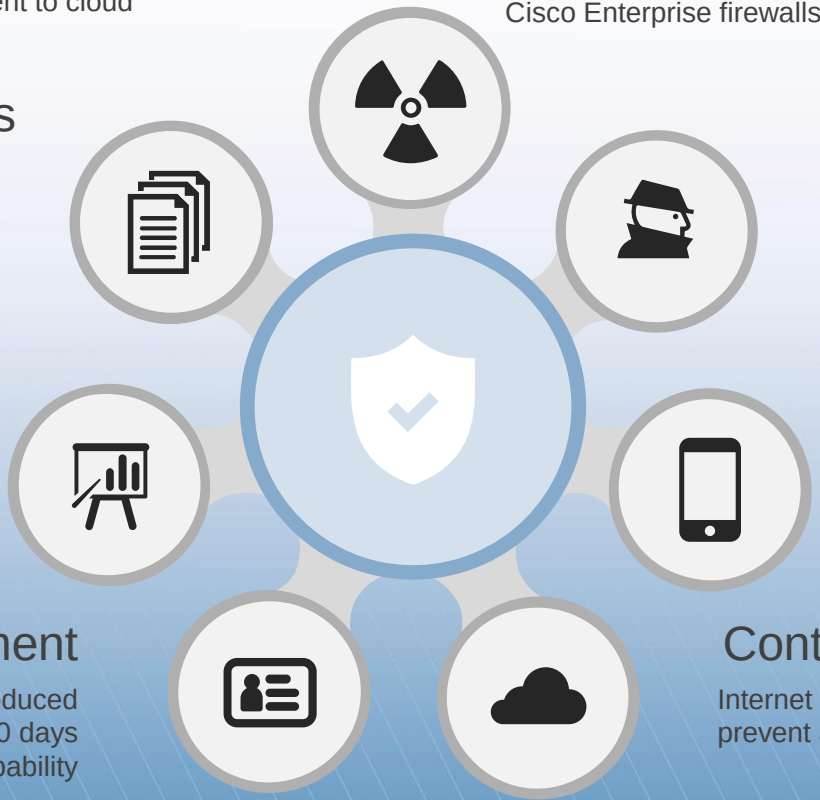
Symantec and Microsoft anti virus
Cisco Enterprise firewalls

Network Access

Advanced Cisco network appliances
Active Directory controls access

Email Filtering

Microsoft email filtering, limit and remove spam, malware, and phishing attempts



Awareness Program

Some phishing training provided to all staff
Regular emails about potential threats

Encryption

Automatic encryption of emails that contain PHI, PII and other identifiers (ZIX)

Password Management

Strong password introduced
Regular forced resets 90 days
Self service reset capability

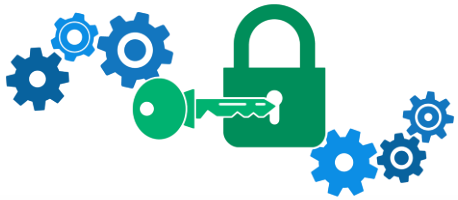
Content Filtering

Internet traffic content filtering, to prevent and reduce malicious sites

OPEN DOOR
FAMILY MEDICAL CENTERS

The Hit!

The Event – 8/26



First Signs

- Users contacts IT Helpdesk
- Some services not connecting
- A few calls only

Investigation

- Troubleshooting of connectivity issues
- Unresponsive or errors on servers
- Many calls received

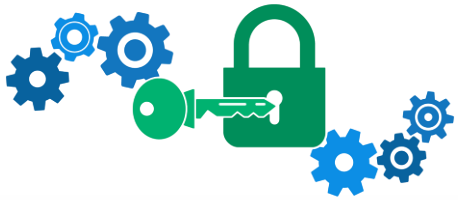
Realization

- File extension has changed
- R3ADME file found
  - Ransom note

Stop the Bleeding

- Cut off the world
- Establish the security incident war room
- Contact cyber security team

Day Zero –
26 August 4am → 12pm



Trick Bot downloaded through phishing email, by 2 Open Door users

2018

First incident reported, as users reported access errors Ransom note discovered

8/26

IT locked down network within 2 hours of incident to prevent further spread and damage

8/26

External Cyber Security Team engaged
Initiated contact with Threat Actors

8/26

Cyber Insurance team contacted, and assigned new Cyber Security Team

8/26

Threat Actors responded with demands.

$

8/26

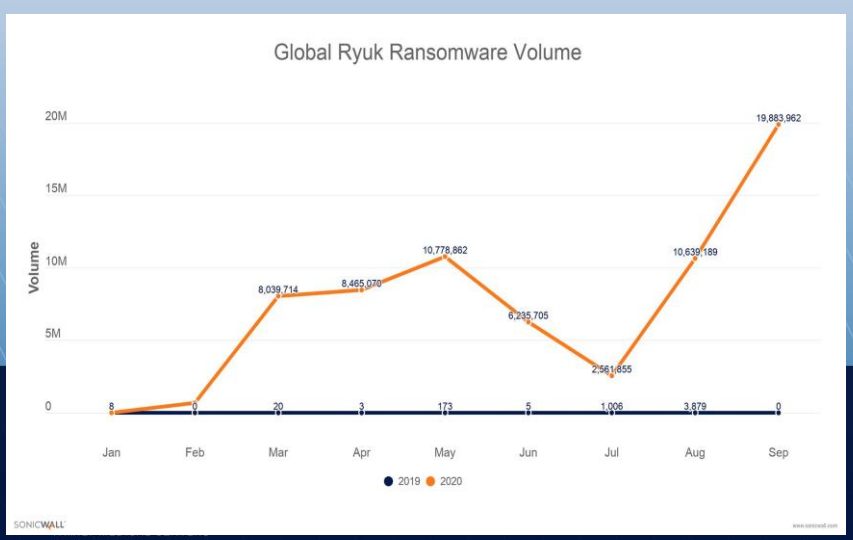
Technical impact assessment started

CONTI ransomware identified

8/26

OPEN DOOR
FAMILY MEDICAL CENTERS

Ransomware



What is ransomware

Delivered through phishing attempts to end users

Ransomware is a form of malware that encrypts files – rendering the machines inoperable.

There are personal and corporate ransomware attacks.

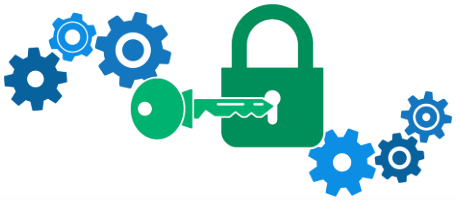
Users are shown instructions for how to pay a fee to get the decryption key.

Threat actors demands a ransom to restore data files (decrypt) upon payment.

The ransom can range from a few hundred dollars to millions, payable in Bitcoin.

The most common delivery method is phishing spam. An attachment sent to a person by email, masquerading as a file they should trust.

Meet CONTI



Conti is being operated by the same group that conducted Ryuk ransomware attacks in the past,

Ryuk is the most active and largest ransomware group in the past two years.

It is almost impossible to determine where threat actors are based.

Ransom is paid in Bitcoins which is literally untraceable

Once ransom is paid, the threat actors will share the decryption key and provide access to the data they might have taken – it can be deleted and **will not** be made public

Changed their tactics – data is taken to extort you!

US Government agencies declares war on cyber crime – 170+ arrests, recovering assets. Stepping up work with industries

Trick Bot was downloaded in late 2018, which was the entry point for the threat actors.

Once in, the bot sat dormant until 26 August when the threat actors kicked off their encryption event.

A ransom note was left on each infected device, stating network had been locked.

Contact details provided using proton emails which is a highly encrypted email service often used by hackers

TrickBot - harvesting emails and credentials. User will not notice any symptoms.

OPEN DOOR
FAMILY MEDICAL CENTERS

Recovery & Impact

Incident Response

Open Door's response process to major incidents
In line with NIST Framework and other security methodologies

Declare Incident

Start Clean-up

Remove the artifacts and clean-up

Finish Clean-up

Restore services and systems

Restore Operations

Report
- Assess
- Address

Identification
- Troubleshoot
- Resolve

Containment
- Prevent spread
- Restrict movement

Eradication
- Rootcause
- Delete
- Remove

Recovery
- Repair
- Rebuild

Lessons Learned
- Process review
- Technology gap
- Skills gap

Cyber Security Consultant

Incident Closed

Communications

Document
Improvements
Policies
Controls
Metrics

OPEN DOOR
FAMILY MEDICAL CENTERS

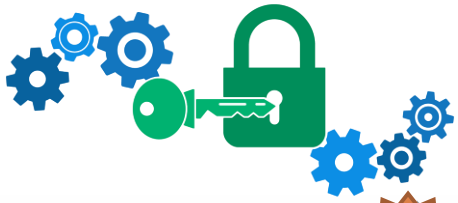
What Do You Need?

A long journey to get fully restored, and depends on critical pieces - It is painful and disruptive, no matter if you rebuild or decrypt!

- Align your IT resources
  - Use skills and staff appropriately
  - Empower them and they will excel
- Cyber Security Insurance
  - Critical to your success
- IT Disaster Recovery Plan
  - Prioritize your applications and services
    - Patient services top priority
    - Payment and HR top priority
- Backup & Restore
  - **Health of back-ups**
  - Test your restore process regularly
  - Build & restore applications servers
- Vendor Relations
  - Build strong – **call in favors**
  - Key to getting systems running faster
  - Short term resources
  - Application install and configuration
- Using the decryption key
  - **80-85% success rate**
  - Servers and computers might not recover
  - File recovery much higher success rate
- Documentation
- Rebuild & Refresh
  - Do both, to be sure
  - 33% of computers significantly impacted
  - 20% of servers could not be restarted
- Assess cloud or on-prem
  - Decide where to rebuild
  - Evaluate cloud and SaaS
    - Move applications to SaaS
  - Consolidate and reduce infrastructure
    - **"Trim the fat"**

Establish a war room!
- Daily meetings
- Track progress
- Communicate

The Recovery Journey



2019 | 8/26 | 8/31 | 9/3 | 9/7 | TODAY | 9/30

Ransom Note

Threat actors encrypts network

Early Recovery

Assess impact and enabling key systems

Priority Systems

Focus on priority systems to get patient services enabled

Decrypt

Decrypt, build and restore services and computers

Forensics

Determine exposure and communications

FBI

FBI

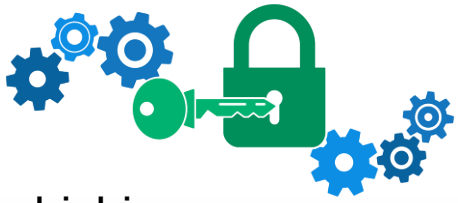
Trick Bot install | R3ADME | Full Outage | Priority Systems | Back-up Health | Build eCW | Solomon Docuware | Decrypt Files | Files and Servers | Data Mining | Media Updates | Operational

Significant Business disruption 8/26 – 9/14

Full Recovery 10/30

OPEN DOOR
FAMILY MEDICAL CENTERS

Assessing the Impact



- Event was triggered by **human interaction** (late 2018) - phishing
- Negotiations lasted for more than 10 days, which is unusual
- Exposure is **minimal** – **some data** exposed
- Significant business disruption for 2 weeks, 4 days without EMR
- Rebuilding EVERY server and computer
  - Recovery Process is slow, and it takes time to restore systems
- **Paying the Ransom?**
  - We did not want to pay!
  - We could restore from back-up
  - Why did we pay? Active Directory and fileserver

98%

Encryption

All files on the network were fully encrypted
Encryption breaks applications
Need decrypt key or back-up

52%

Damage

20% of servers cannot be restarted
36% of computers cannot be used

1.5%

Data "Loss"

Threat actors 'only' downloaded 4GB of data - Data was returned
Data mining underway

OPEN DOOR
FAMILY MEDICAL CENTERS

My Verdict

My IT team responded well to the event, considering the circumstances, but it did expose some weaknesses that needs to be addressed. Mainly process and system enhancements.

Staff were updated several times during the day and week(s); email and the intranet

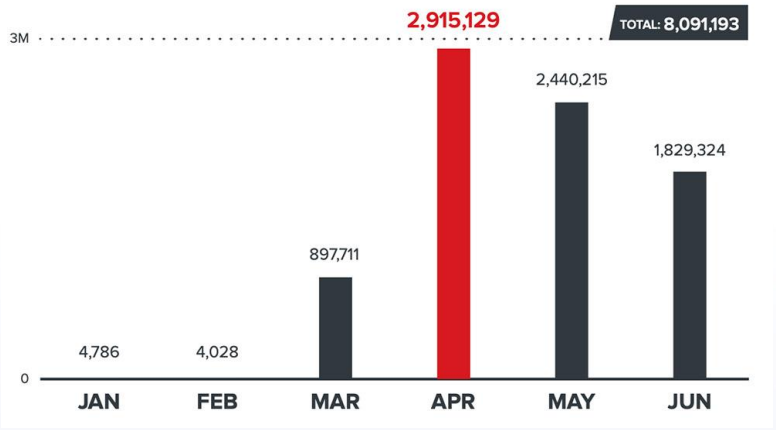
Conduct IT self assessment, post mortem – learn from this event

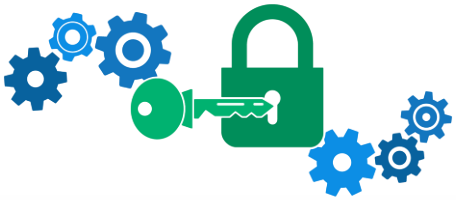
Our network is state of the art – and many security tools running to protect us

Technology can help us most of the way, but human interaction is hard to safeguard

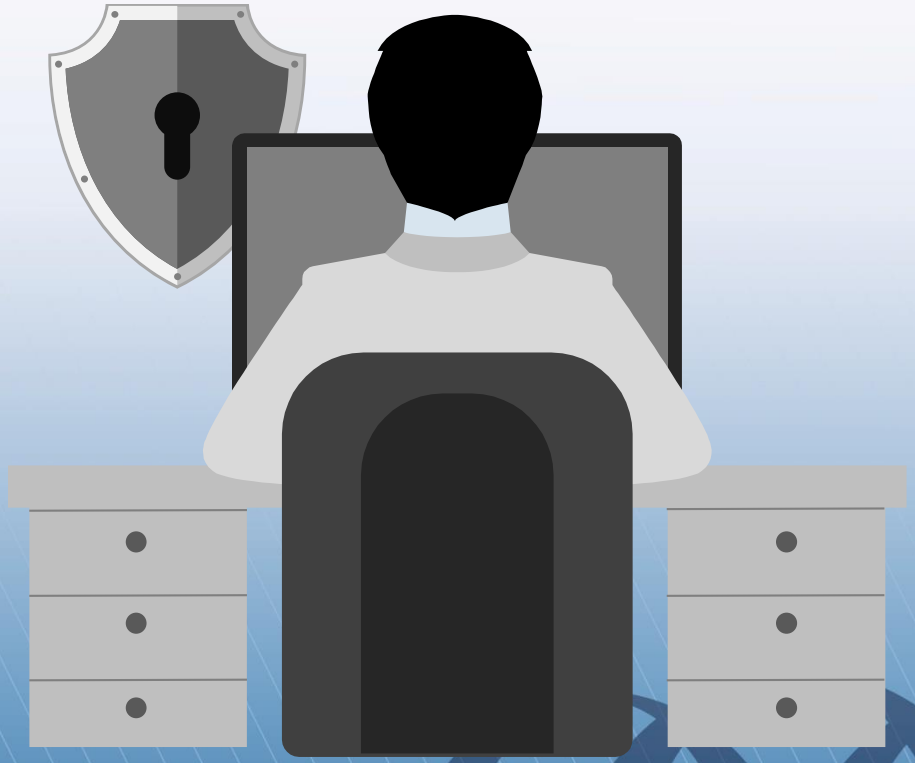
- Build a 3-year IT & Security roadmap
  - Eliminate ageing and vulnerable systems
  - Cloud enablement – **Cloud First**
    - HIPAA compliant
    - Move applications to our cloud
    - Replace systems that does not support cloud
  - Ensure systems and sites are redundant
    - Setup and **test fail-over**
    - Eliminate network bottlenecks and complexity
  - Fully document server and application architectures
- Conduct annual security assessments
  - NIST Framework
  - Vulnerability and penetration
- Investing in enterprise tools and outsource monitoring services
  - Email filtering
  - Back-up strategy
    - Storage & Retention policy
- Enhance **end-user awareness** and access their technology
  - Computer locks
  - training & awareness, USB devices, etc.
- Build the cybersecurity framework - **hire a resource** to manage this
- **Security measures will disrupt!**
- Train IT in ITIL – providing a structured approach for our service management
- Implement cyber security program
  - NIST Framework
  - Web site

OPEN DOOR
FAMILY MEDICAL CENTERS



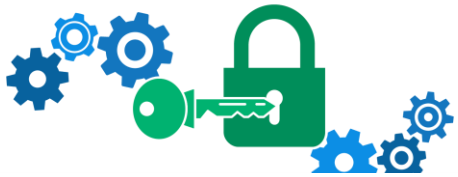


The Future



OPEN DOOR
FAMILY MEDICAL CENTERS

Technical Enhancements



Multi-Factor Authentication

Only allow users to connect to Open Door if they use secure methods; VDI/MFA or VPN/MFA

- ✓ Industry standard and mandatory
- ✓ Pin based approach to mobile devices

Enterprise E3 Licenses

- License compliance
- Local firewalls and defender
- Multi-factor, email DLP
- ***Cloud based***

Cynet

- ✓ Enterprise anti virus / EPP
- ✓ AI for patterns and unusual behaviors
- ✓ Active scanning devices
- ✓ Quarantine and block known threats
- ✓ Updated centrally based on security world
- ✓ ***Cloud based***

eCW Faxing

- Remove loss of important patient faxes
- Integrated with eCW
- Cost reduction – remove 13 lines
- ***Cloud based***

Voice & Data Consolidation

- ✓ Reduce lines into sites and data centers
- ✓ Leverage enterprise services
- ✓ Dedicated lines for data and voice

Cisco Backbone

Hardware ***DONE***	State of the art network and perimeter fences
SDWAN ***IN PROGRESS***	Highly secure network traffic management

Firewalls

- Cisco gear – integrated with Cisco Backbone
- Intrusion Detection
- Content filtering
- Replace zScaler

Mimecast Filtering

- Eliminate phishing, impersonation and ransomware
- Protects against malicious web activity
- Detects and responds to cyber attacks
- ***Cloud based***

Preparing for the future

- ✓ Building a SOC/NOC capability
- ✓ Implement NIST Framework & Cybersecurity Committee
- ✓ Improve and secure 3rd party connections
- ✓ Cloud first strategy (cloud, SaaS, etc.)

Email Encryption

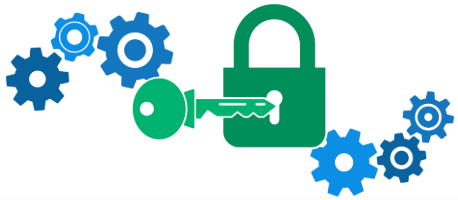
- Force encryption of all emails containing PHI, PII and other sensitive data
- Replace ZIX with Mimecast

Enterprise Back-up Restore

- Small on-prem back-up appliance
- Ransomware prevention
- Disaster recovery / fail-over
- Manage on-prem and cloud data, and email
- ***Cloud based***

Open Door
Family Medical Centers

Security Measures



User Interface	The Perimeter	Monitoring	Awareness
• Lock down desktop settings • USB drives • SPAM filters • Less applications installed • Stricter install • File and computer inspections	• Reduce external connections • VPN / VDI / MFA • 3rd party connections • SPAM filtering • DDOS readiness • Real-time EPP and IDS	• Firewall perimeter alerts • Enable IPS on firewalls • Operations Center – central interface with key systems and alerts • Back-up & Restore process • 3rd party security monitoring	• Security incident process • Awareness emails • Security web site • Targeted campaigns • Monthly newsletters • Quarterly IT Townhall?

SECURITY FRAMEWORK

Cybersecurity Committee	Oversee our compliance, security and audits	Program based on standards will ensure full compliance. Internal audits	New framework and standards (e.g. HIPAA). Document policies and procedures.	Annual risk, security and compliance training. Organizational awareness.	Executive dashboards and KPIs, and compliance. React and adjust.

OPEN DOOR
FAMILY MEDICAL CENTERS

Cybersecurity Committee

Establish the Cyber Risk Committee to oversee, evaluate, and monitor all Open Door's **cyber-risk management** activities

Provide **oversight responsibilities** regarding Open Door's company-wide security and enterprise risk management practices, including;

1. Promote a culture with a secure mindset
2. Manage policies, procedures, and controls
3. Mitigate risks related to cyber security
4. Evaluate and review privacy of staff, company and patient data
5. Owning the business disaster & recovery plan
6. Review technologies used to protect Open Door network, data, patients and staff

The Committee will **manage and mitigate cyber-risks** related to strategic, commercial, physical security, legal, regulatory, and reputational.

Lead the **implementation of the NIST Framework** to ensure policies, procedures, and controls are in place, as well as conduct regular checks and audits.

Provide reports and updates to the Executive Board on an annual basis, and if events occur.

Cyber-Risk Spheres at Open Door

Physical Security
- Physical Access
- Cameras
- Facility Health
- Perimeter and access reviews

Information Technology
- System availability
- Security Incidents
- Metrics & Dashboard
- Proactive monitoring

Policies & Procedures
- Security assessments
- Security Framework
- Disaster Recovery & Contingency
- Audit and mitigating controls

Committees
- Risk committee
- EOC
- Joint Commissions
- RMS

Stakeholders and Contributors

OPEN DOOR
FAMILY MEDICAL CENTERS

NIST Framework

What is NIST

National Institute of Security & Technology - The NIST Framework is based on existing standards, guidelines, and best practices for organizations to better manage and reduce cybersecurity risk.

It is a widely used and recognized standard that supports HIPAA compliance, and applied within healthcare industries.

- Annual security assessment conducted by Health Efficient (FOC), in Nov' 2019, and Nov' 2020, are using NIST
- Technical penetration & vulnerability assessment carried out in 2018, and in Nov' 2020, are using NIST

Using NIST will require a framework owner, who can identify and manage the processes. This person will not be responsible for documenting, but to ensure that it gets created and communicated.

Open Door's Security Framework delivers a mature tool to document, track and implement tighter controls, and complete audits validating that our risks are managed.

- Set of desired cybersecurity activities and outcomes
- Manage and reduce cybersecurity risks
- Establish a cybersecurity program; risk, mission priority, and budget
- Identifying and prioritizing opportunities for improving cybersecurity
- Build awareness within Open Door, and our stakeholders

Audits are conducted throughout the year to measure maturity, compliance, and ensure policies/procedures are reviewed annually.

The Open Door Security Program will outline all activities and made available to all staff.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO