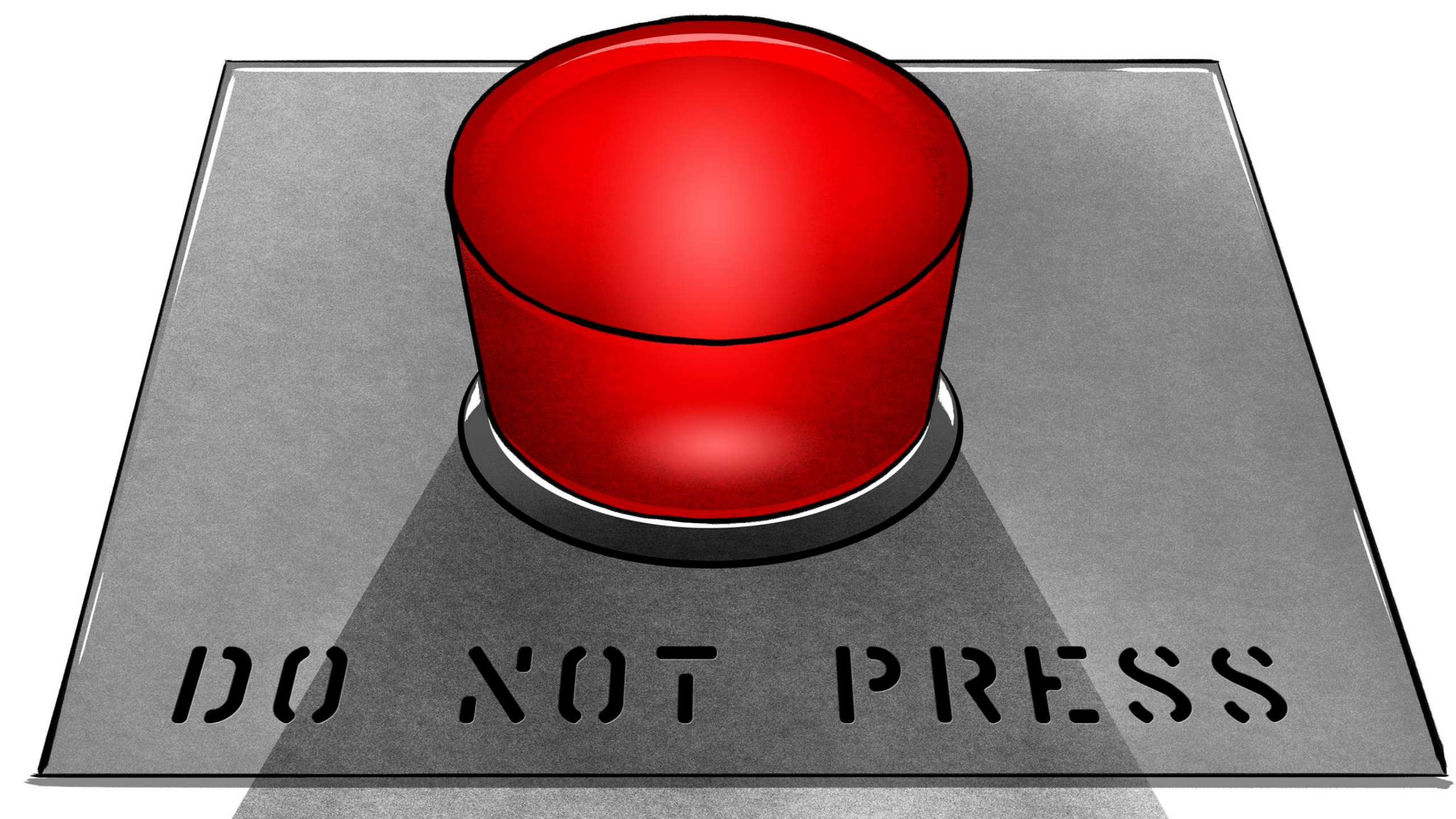
Waterfall Security Solutions

Unbreachable protection
Unlimited connectivity

Tjeerd Zwijnenberg – Sales Director Europe
E: tjeerdz@waterfall-security.com M: +31621979091

Industrial Cyber Security
10 oktober 2023 | Congrescentrum 1931, den Bosch


DO NOT PRESS

SECURE OPERATIONS TECHNOLOGY

IT-SEC:

protect the information

SEC-OT :

protect physical operations *from* the information

Stop **bi-directional** communication between the criticality boundaries

waterfall

In almost all physical operations, the goal is **Safe**, **Reliable**, and **efficient** operations, almost always in that order.

"You cannot restore human lives, damaged equipment, or lost production from backups"

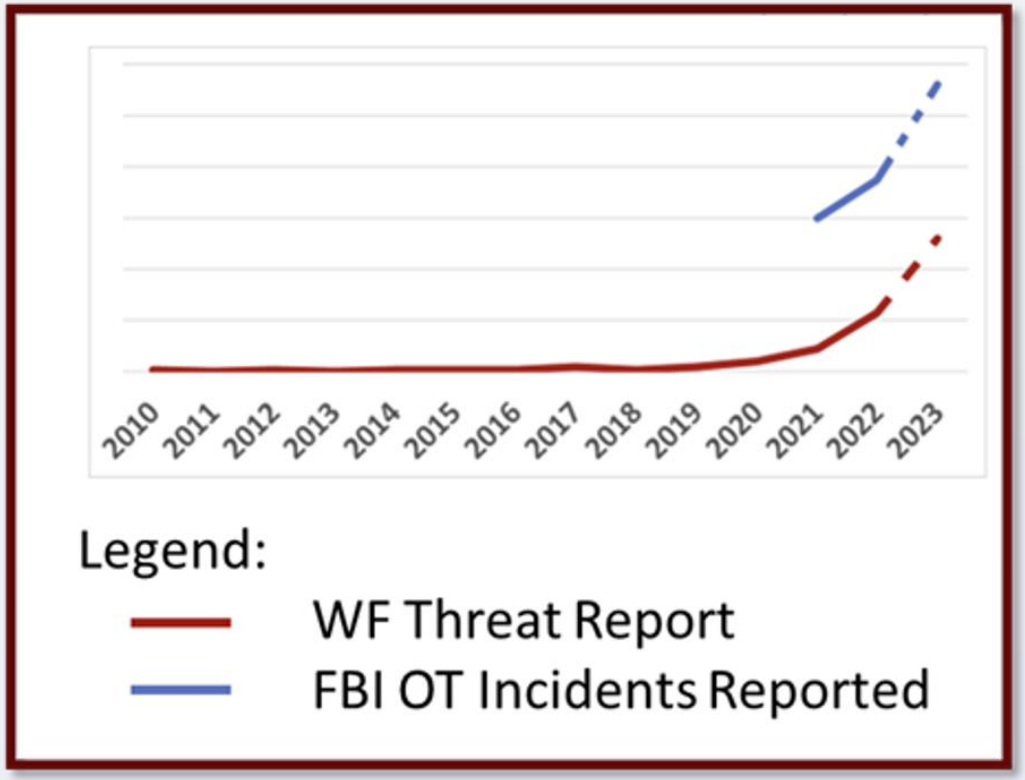
OT CYBER RISK – CHANGED FOREVER

EXPONENTIAL GROWTH & STATE CHANGE

- From "*theoretical possibility*" to "*real*"
- Growing exponentially
- Use of nation-state tools & techniques

ALMOST ALL RANSOMWARE – HOW?

- Some ransomware targets OT specifically
- Some victims stop OT in "*abundance of caution*"
- Some OT systems fail because of OT -> IT dependencies



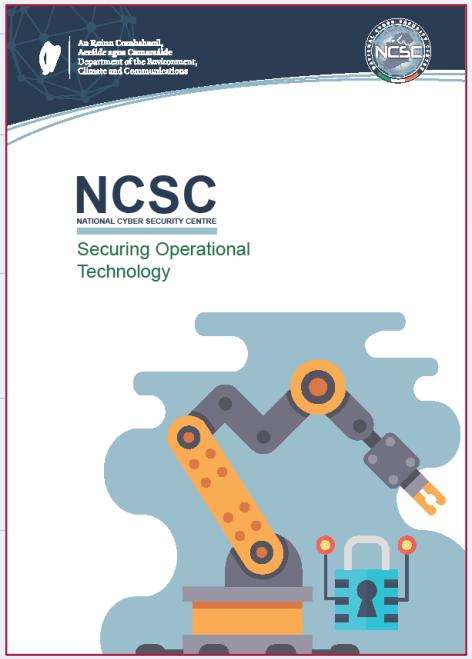
At 150% annual growth, we will see 4,500 attacks in 2027 affecting 15,000 sites

waterfall

NCSC OT Cyber Guidelines

NCSC directives indicate that you need to assume that your corporate or any external network is being compromised.

1. Stronger perimeter controls for "**Segmentation & Isolation**" of critical networks at the critical boundaries & **Network & System Hardening**
2. More secure **Control Access to the Network** (Remote Access)
3. Improve **Cyber Incident Response** (IDS/SIEM/SOC)
4. Vulnerability & **Patch Management**
5. **Log Management** & Analysis



Secure Operations Challenges

Unacceptable risk vs. Business need

Industrial cloud services

Vendor monitoring

OT visibility

Patch & Virus Management

Recipe & Document Management

Remote Access

Targeted ransomware

DOS attack

Phishing

Unacceptable Risk

- Cloud connectivity increases exposure
- Safety & equipment protection concerns
- Engineering change control limits options
- Physical consequences of compromise

Vs.

Business Need

- Predictive maintenance & big data analytics
- New automation visibility into OT
- Compliance with enterprise security program
- Increased efficiency and agility

waterfall

What is a “Red Button” or “Cyber Kill Switch” in OT?

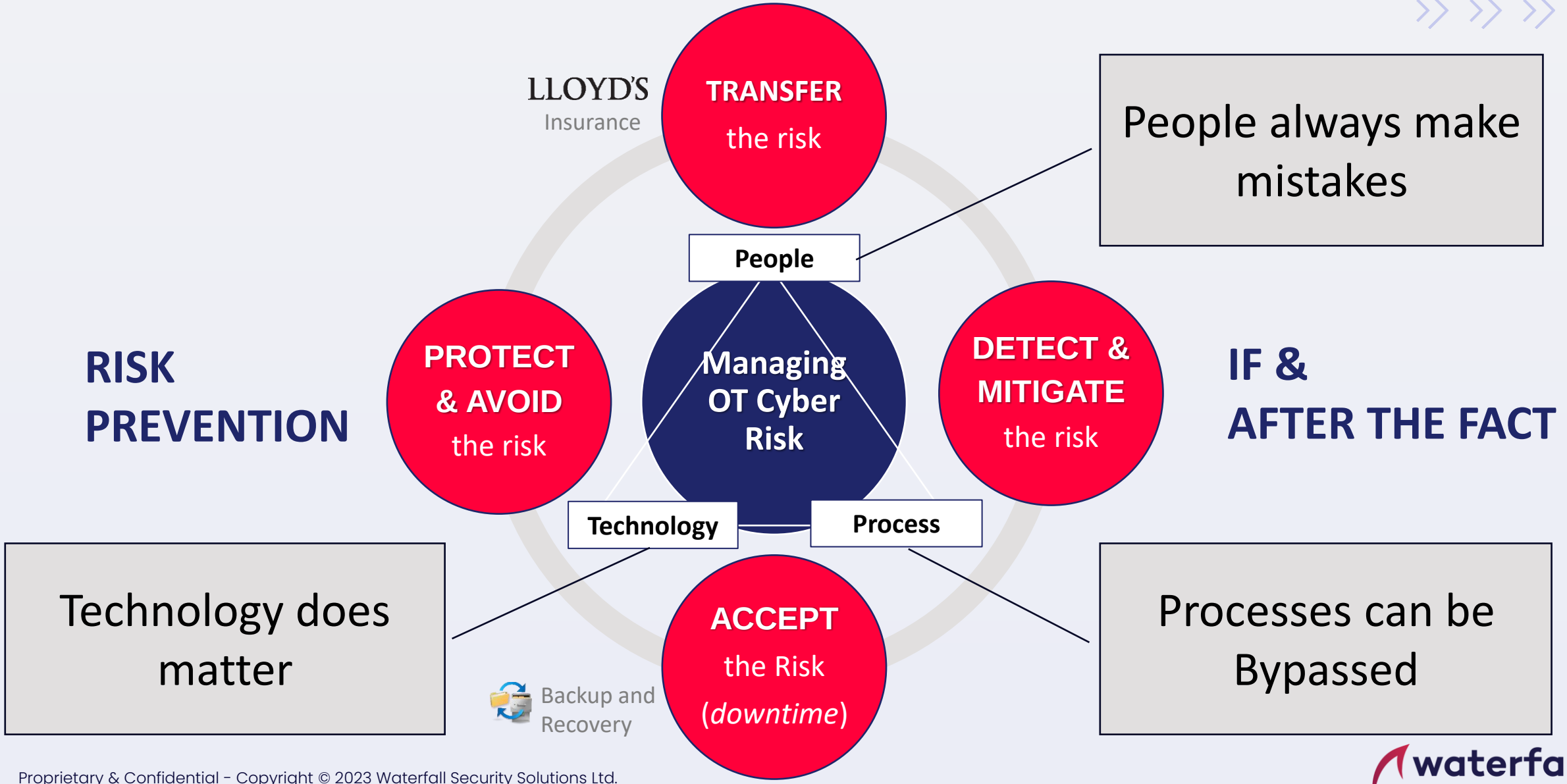
Red Button

“A manual button which people in either OT or IT can push to physically disconnect the OT networks from the internet (IT/Cloud) in the event of a serious attack”

Both mechanisms are **REACTIVE** and **MANUALLY** activated and put OT in “**Islanding Mode (Air-gapped network)**”.

- Are you sure you will detect?
- How fast can you disconnect the network?
- How long can you continue without access to OT data?
- How long can your people run the plant manually?

PILLARS for OT CYBER SECURITY



waterfall

Engineering Grade Solutions

- Are Physical and cannot be breached
- Are **Deterministic** and **Predictable**
- Go beyond the traditional cyber security strategies
- Best way to stay ahead of the threat
- Help solve “Abundance of Caution”
- Provide **100% protection** to you critical OT environment against outside attacks from IT/Cloud
- Provide Real-time access to all your OT Data outside the OT Domain with highest Data Integrity

ALL SOFTWARE CAN BE HACKED

All information flows are attack vectors

Focus on physical, not software protection, against cyber attacks

Software Alone is not Enough

Firewalls
Firewalls are *100% software* and *bi-directional* – all software has vulnerabilities. Layers of firewalls are porous and are routinely breached.

OT IDS
Intrusion Detection Systems detect attacks *after* they happen and *if* they detect

Identity and Access Management

Protects against unsophisticated insiders, not professional-grade criminals or other attackers

- you need to assume that your login credentials are hacked -

Updates & patches

Continuous, time consuming & sometimes introduce new vulnerabilities

- we live in a world where software is not bug free anymore – time patch? -

Unidirectional Security Gateways

Absolute protection with complete network visibility

Absolute protection - The gateway hardware is physically able to send information in only one direction

Network visibility - The software makes real-time copies of servers & devices from the industrial network to the enterprise network, and IT users access the replicas normally"

No attack - No matter how sophisticated, attacks cannot propagate back to the industrial network through the gateway

BUT I NEED INBOUND DATA

…. what risk are you willing to accept?

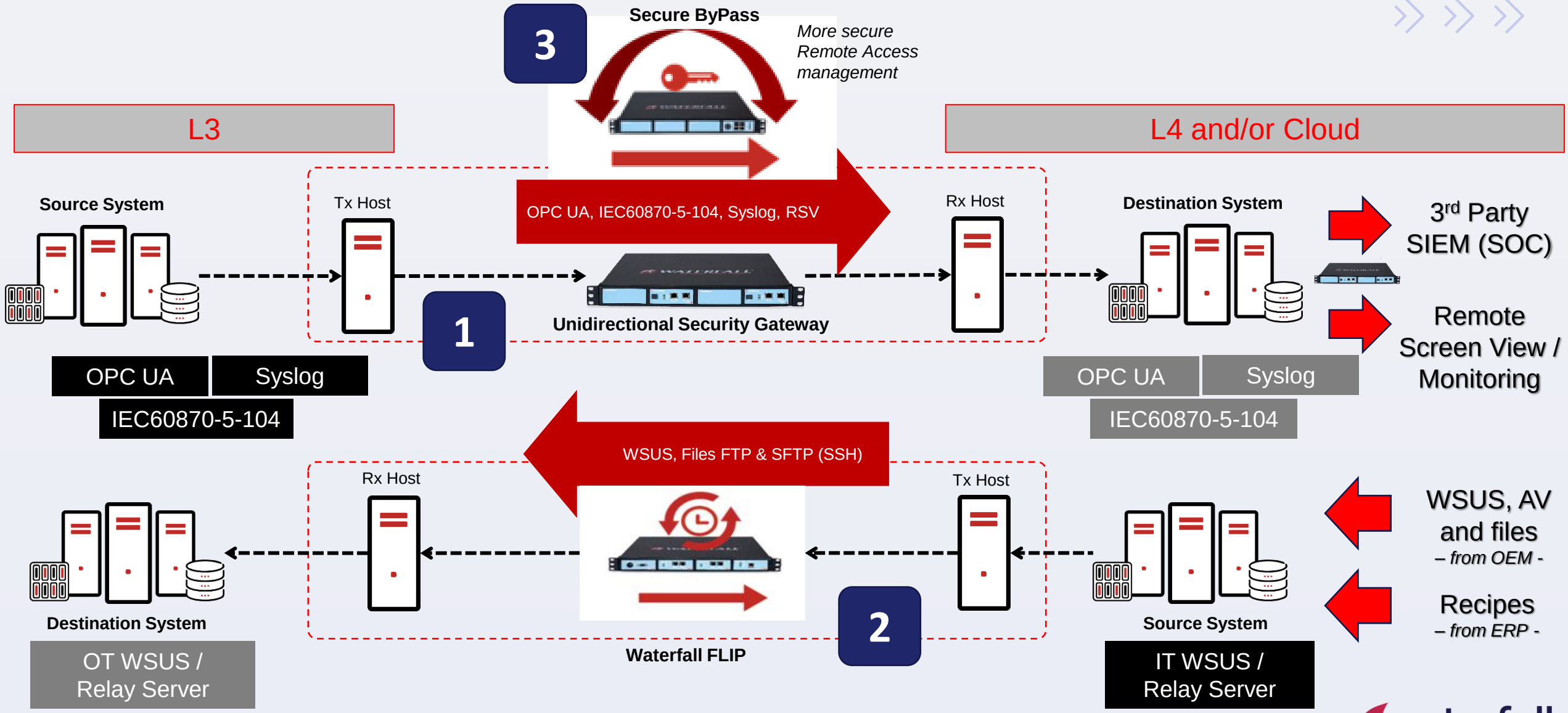
Did you know that two-way unidirectional communication is not bi-directional and has no closed loop?

Outbound (OT > IT)

Inbound (IT > OT)

waterfall

Example Customer



Jump AHEAD of the Threat

- **Attacks only get smarter** but all attacks are information – if we control the flow of information, we control the attacks
- **Protect OT now** Consequences of compromise range from costly to unacceptable
- **Unidirectional security gateways** provide absolute protection against even the most sophisticated attacks

SEC-OT best practice

At least one layer of unidirectional protection significantly enhances OT security, defending against both current and future threats.

waterfall

About Waterfall Security

2007
Founded

>1000
Sites

>20
Verticals

6
Global Sales & Ops Hubs

14
Published Patents

Member of:

EE-ISAC

EUROPE HQ (Netherlands)
UK, Netherlands, France, Germany, Switzerland, Norway, Sweden, Finland, Iceland, Denmark, Baltics, Spain, Italy, Portugal, Greece, Poland, Romania, Ukraine, Kazakhstan, Poland,, ….

Leading the world's OT unidirectional gateway market with superior solutions, worldwide presence, and proven track record of success

Key Sectors:

Power | Oil & Gas | Rails | Facilities | Water | Manufacturing | Government

waterfall

Thank you

Waterfall European HQ

1. WF Intro & Use case gathering session
2. Executive Briefing
3. Workshop & Demo
4. Blueprint Architecture Workshop
5. Integration Testing for OEM and Technology Partners

Europe Office

Barbara Strozzilaan 201,
1083 HN, Amsterdam.
Netherlands
+316-21979091

Waterfall Software Connectors

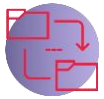
Historians & databases

- Aveva (OSIsoft): PI, PI Asset Framework, PI Backfill
- GE: iHistorian, iHistorian Backfill, OSM, Bently-Nevada System1
- Schneider-Electric: Wonderware eDNA, Wonderware Historian, Wonderware Historian Backfill, SCADA Expert ClearSCADA, Siemens CFE & WinTS
- Rockwell FactoryTalk Historian , Honeywell Alarm Manager
- AspenTech IP.21, Scientech R*Time, Microsoft SQL Server, Oracle, MySQL

Industrial applications and protocols

- Siemens S7
- Yokogawa ExaQuantum OPC, GE iFix, Leidos HBS
- OPC DA, A&E, HDA, HDA Backfill, OPC UA, UA Historians, UA Alarms & Events
- Modbus, DNP3, ICCP, IEC 60870-5-104, BACNet IP

File transfer



- Folder mirroring, Local Folders
- FTP/S, SFTP, TFTP, CIFS, SMB, NFS
- Remote Folder Transfer

Enterprise monitoring

- FireEye CloudConnect, Email/SMTP, SNMP, Syslog UDP/TCP, TCP/IP & Multi, UDP
- HP ArcSight SIEM, McAfee ESM, Splunk, Qradar
- CyberX (Microsoft), Helix & Managed Defense, Dragos, Indegy, Radiflow iSID, Ethernet Spoofing, ForeScout Silent Defense,
- MSMQ, IBM MQ, Active MQ, AMQP, TIBCO EMS, MQTT, RabbitMQ, HTTP-Request, Kafka
- SolarWinds Orion, Emerson EDS,

Remote access

- Remote Screen View
- Secure Bypass

Other connectors

- TimeSync, Netflow
- Video & audio streaming, Broadcast, Multicast
- WSUS updaters
- AV Updates
- Remote printing, Rsync

waterfall

Data Integrity Features & Options

High quality optical hardware – does not lose bits

Forward error correcting codes – like Hamming codes – more efficient

Retransmissions Able to send each message many times, duplicates discarded

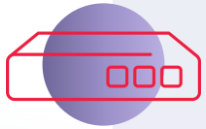
Sequence numbers & heartbeats – prompt error detection

Buffers and queuing at every stage of the transmission pipeline

Backfill – manual retransmission

High availability – no single point of failure

In practice, less than 5% of customers buy high availability – the systems are that reliable



waterfall