Innovation Talk

Securing Critical Infrastructure

How to be effective about protecting your OT environment

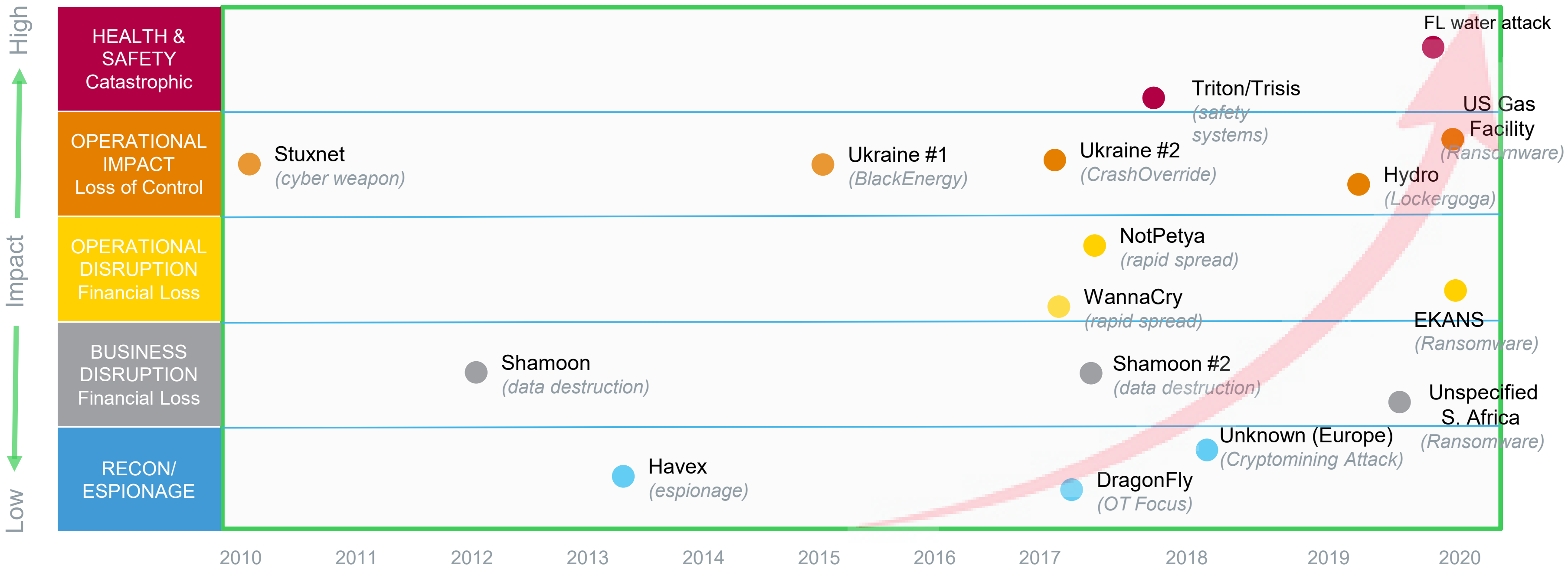
Life Is On | Schneider Electric

IT vs. OT

- Enterprise system and networks used to manage IT process and data that support banking systems, personal devices (laptops, cell phones, etc.)
- Focus area - confidentially
- Data Confidentiality, data integrity and operational continuity are the priorities.

- Operational networks that support that control physical processes such as Oil & Gas, Water, Mobility, Building Management Systems, etc.
- Focus areas – availability
- Operational continuity and safety of humans and environment are the priorities.

The Evolving OT Threat Landscape



OT attacks are increasing in both frequency and impact

What kind of Damage do Cyber Attacks do?

Every **11** sec a ransomware attack occurs

Within **5** min the average time it takes for an IoT device to be attacked after going online

21 days Average amount of downtime caused by cyber attack

$200k Average ransom fee in 2021 (up from $5k in 2018)

$40M Largest ransomware payout in 2021

60% Of respondents experienced a revenue loss from a cyber attack

53% Of respondents experienced damage to their brand / reputation

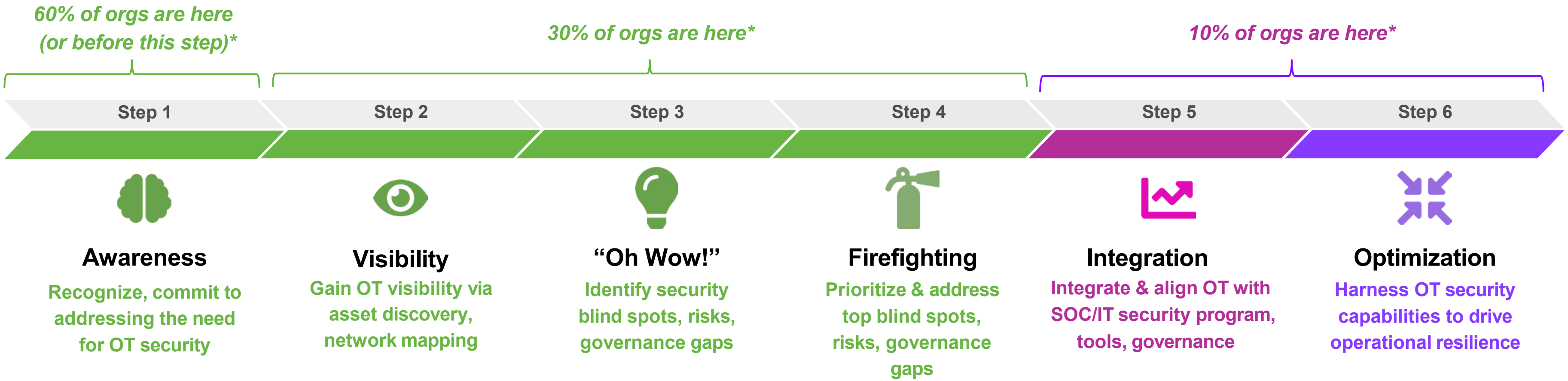
29% Of respondents had to reduce workforce after a cyber attack

42% Of companies w/ cyber insurance indicated that insurance only covered a small part of damages

600% Growth in amount of malware sent via email during COVID

Source:
ABC News, Cybereason, Business Insider, CISA, Acronis, Hashed Out

OT Cybersecurity Maturity Map



*60% of orgs are here (or before this step)**

*30% of orgs are here**

*10% of orgs are here**

Step 1

Awareness

Recognize, commit to addressing the need for OT security

Step 2

Visibility

Gain OT visibility via asset discovery, network mapping

Step 3

"Oh Wow!"

Identify security blind spots, risks, governance gaps

Step 4

Firefighting

Prioritize & address top blind spots, risks, governance gaps

Step 5

Integration

Integrate & align OT with SOC/IT security program, tools, governance

Step 6

Optimization

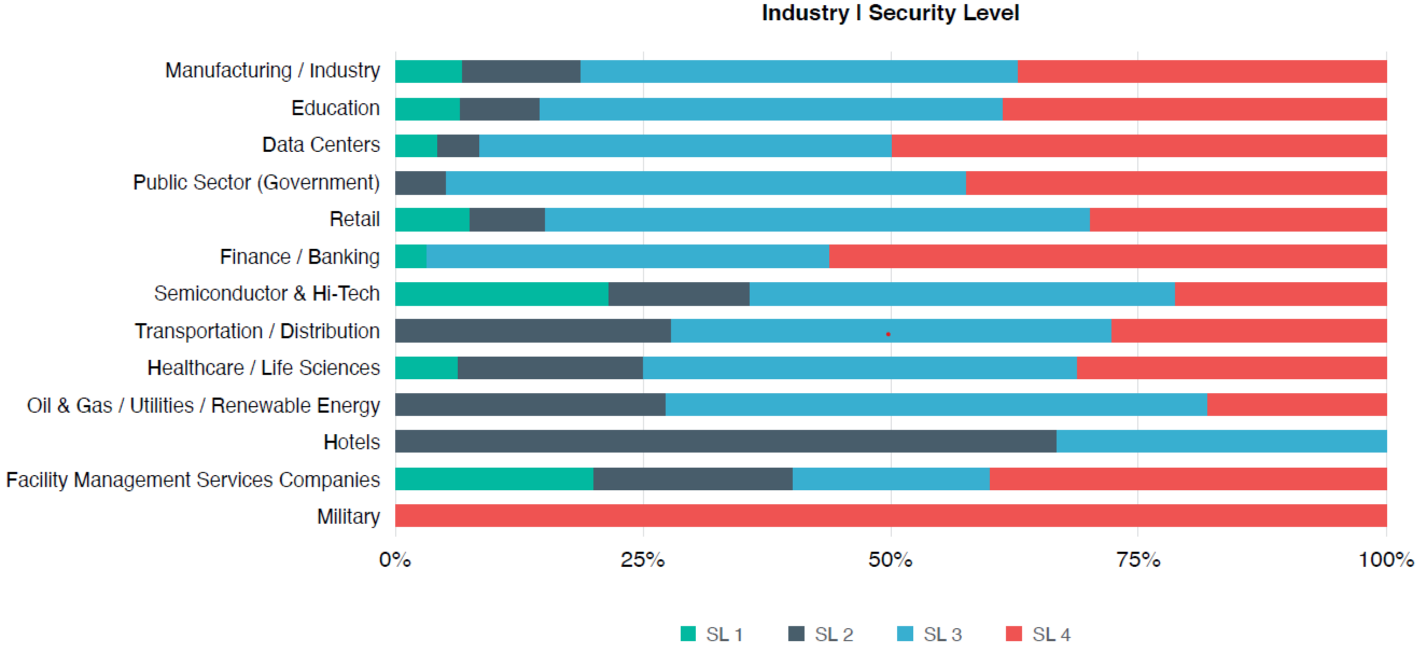
Harness OT security capabilities to drive operational resilience

The minimum is not enough – customers are asking for SL3 & SL4

425

Respondents

- **Geographies:** US, UK, France, Spain, Germany, Italy
- **Industries:** Manufacturing, Education, Data Centers, Public Sector, Retail, Finance/Banking

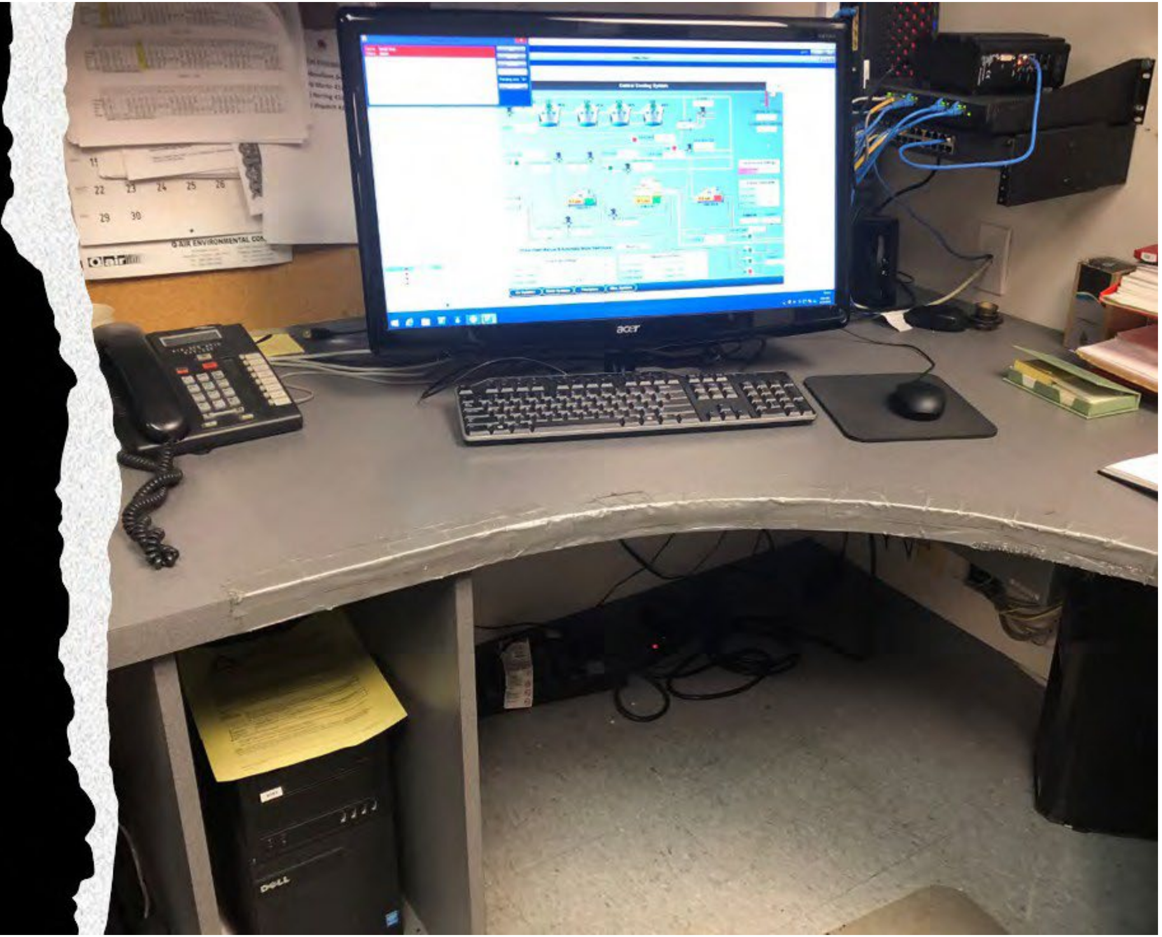


ProfitWell 2021

Life Is On Schneider Electric

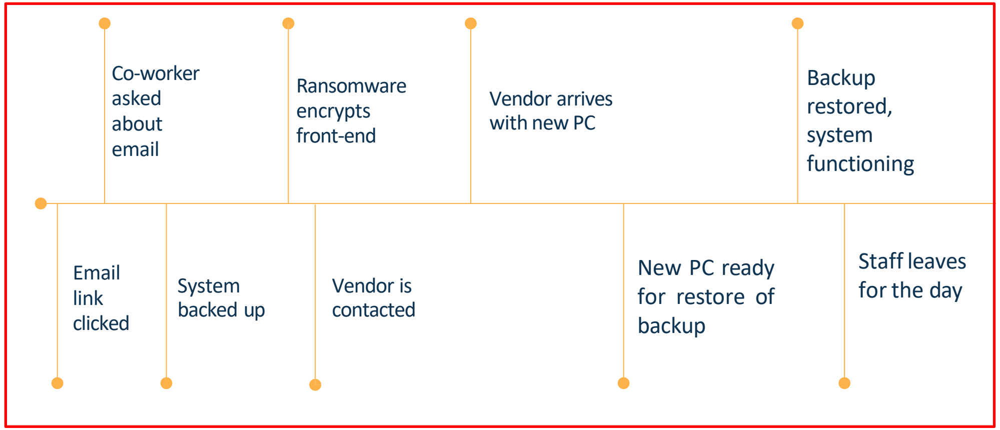
Timeline of a Cyber Attack (and recovery)

HVAC System



Timeline of Events – Day 1…

Day 1



Email link clicked

Co-worker asked about email

System backed up

Ransomware encrypts front-end

Vendor is contacted

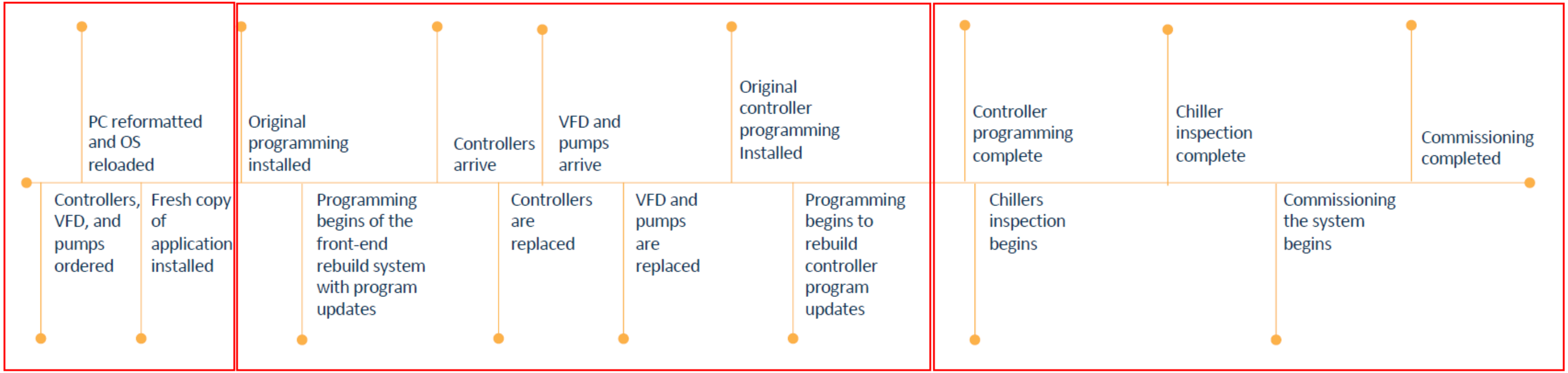
Vendor arrives with new PC

New PC ready for restore of backup

Backup restored, system functioning

Staff leaves for the day

Timeline of Events – Day 2 +…



Day 2

Controllers, VFD, and pumps ordered

PC reformatted and OS reloaded

Fresh copy of application installed

Day 3 thru 42

Original programming installed

Programming begins of the front-end rebuild system with program updates

Controllers arrive

Controllers are replaced

VFD and pumps arrive

VFD and pumps are replaced

Original controller programming Installed

Programming begins to rebuild controller program updates

Day 43 thru 92

Controller programming complete

Chillers inspection begins

Chiller inspection complete

Commissioning the system begins

Commissioning completed

Why are Operational Cybersecurity Attacks so Successful?

- Vast amounts of high value IP, low tolerance for downtime

  Companies spend millions *(or more!)* developing and modernizing their infrastructure – loss of IP can have substantial impact on revenue and growth.

- Tampering with equipment has long-reaching impact

  If a device is hacked, entire facilities may need to be inspected or reprogramed. In the best case, this causes lost time and revenue – but could also cause safety impacts and loss of reputation/trust.

- High levels of regulation and public scrutiny

  Cyber attacks can impact SLAs and Regulations, which lead to fines and investigations.

- Mixed vendor and maturity infrastructure

  Most facilities have a mix of equipment brands, ages, protocols…all of which create risk and add complexity to effective asset and lifecycle management.

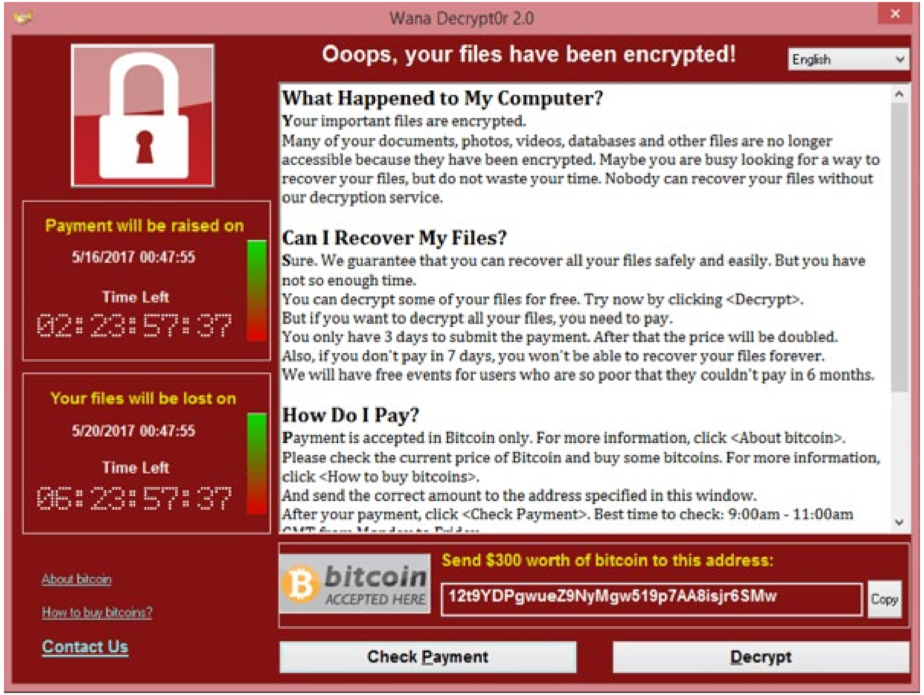
What is RANSOMWARE?

> **Ransomware –** malware/“bug” that employs encryption to hold a victim’s information at ransom

- Users cannot access files, databases, or applications – both IT and OT (Operational Technology).
- Automatically spreads across an entire network, database, database and file servers
- Victim must pay to receive a “decrypter,” which is not guaranteed to work (especially in OT).

> **RaaS –** Ransomware as a Service

- “Malware Service” model that allows ransomware developers to sell their automated creations for users to deploy on victims.
- Usually has a paid subscription / support model
- Non-technical criminals buy their wares and launch the infections, while paying the developers a percentage of their take



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Life Is On | Schneider Electric

Why is Ransomware so effective?

- Recognized risk factor

  Operational systems are now more widely recognized as an attack target in respect to safety and production – there's more risk, and thus more pain, and more ***money*** for attackers.

- Low Risk for Attackers

  Ransomware (and crypto payments) are nearly impossible to trace, and there are multiple levels of separation between the developers and the users of the tools.

- New Age of Threats

  Ransomware tools are becoming more advanced, easier for the non-technical user to deploy.

- Shortage of Qualified Employees

  A scarcity of qualified resources with cybersecurity expertise in Operations means that organizations can't keep up with the tools, technologies, and processes needed to combat.

How does Ransomware get into a network?

- Credential Scraping

  Identifying a user's login information to access the system in an authorized way.

- Phishing Messages

  Malicious emails / links disguised as legitimate messages

- Infected Websites ("Drive-by Downloading")

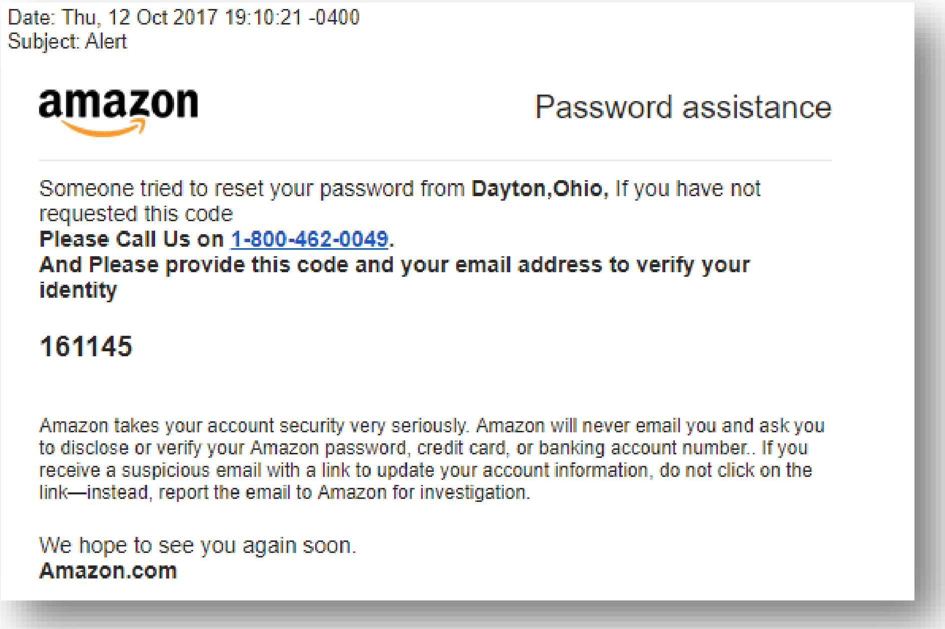
  Unknowingly visiting a website with infected code, where malware is downloaded and installed without the user's knowledge.

- Sale of Classified Information

  Dark web forums have auction houses to buy/sell legitimate company credentials

How does Ransomware get into a network: **CREDENTIAL SCRAPING**

How does Ransomware get into a network: **PHISHING MESSAGES**



Date: Thu, 12 Oct 2017 19:10:21 -0400
Subject: Alert

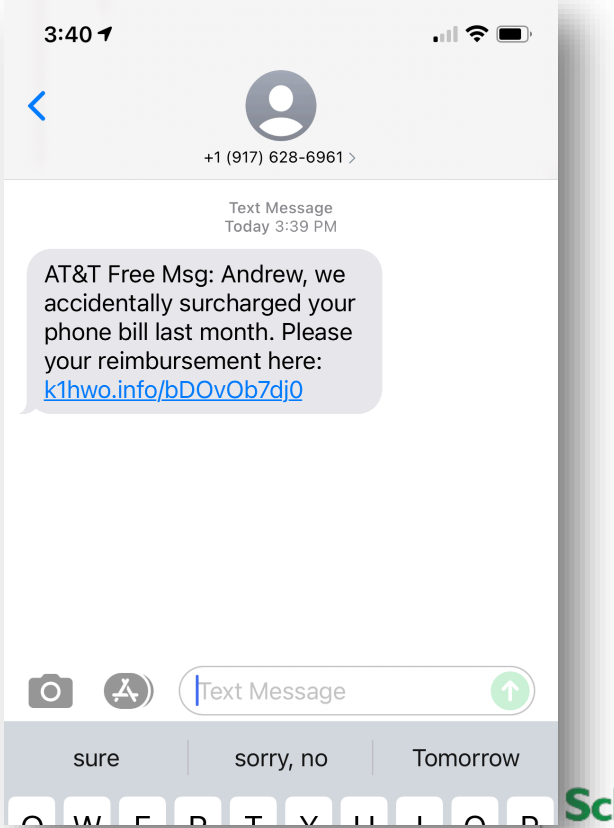
Password assistance

Someone tried to reset your password from **Dayton,Ohio**, If you have not requested this code
Please Call Us on 1-800-462-0049.
And Please provide this code and your email address to verify your identity

161145

Amazon takes your account security very seriously. Amazon will never email you and ask you to disclose or verify your Amazon password, credit card, or banking account number.. If you receive a suspicious email with a link to update your account information, do not click on the link—instead, report the email to Amazon for investigation.

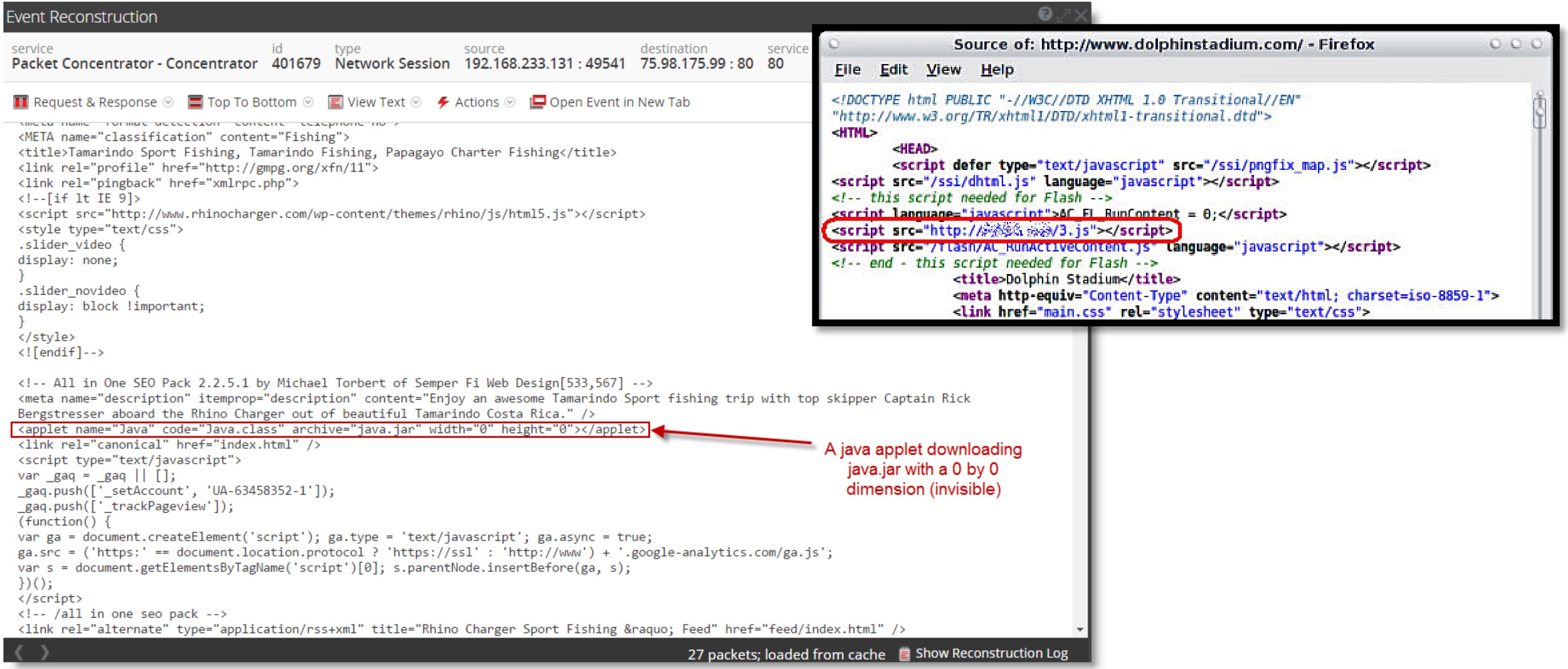
We hope to see you again soon.
Amazon.com



Text Message
Today 3:39 PM

AT&T Free Msg: Andrew, we accidentally surcharged your phone bill last month. Please your reimbursement here: k1hwo.info/bDOvOb7dj0

How does Ransomware get into a network: **INFECTED WEBSITES**



service	id	type	source	destination	service
Packet Concentrator - Concentrator	401679	Network Session	192.168.233.131 : 49541	75.98.175.99 : 80	80

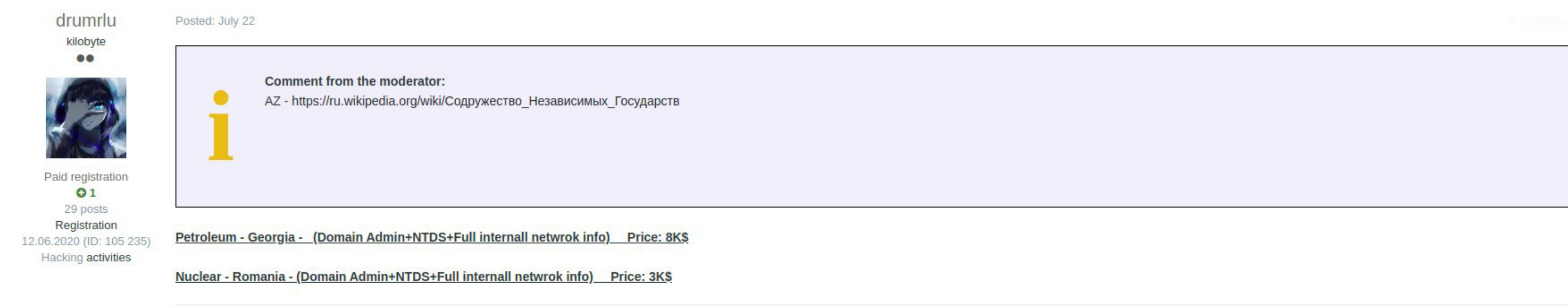
```
<meta name="format-detection" content="telephone=no">
<META name="classification" content="Fishing">
<title>Tamarindo Sport Fishing, Tamarindo Fishing, Papagayo Charter Fishing</title>
<link rel="profile" href="http://gmpg.org/xfn/11">
<link rel="pingback" href="xmlrpc.php">
<!--[if lt IE 9]>
<script src="http://www.rhinocharger.com/wp-content/themes/rhino/js/html5.js"></script>
<style type="text/css">
.slider_video {
display: none;
}
.slider_novideo {
display: block !important;
}
</style>
<![endif]-->

<!-- All in One SEO Pack 2.2.5.1 by Michael Torbert of Semper Fi Web Design[533,567] -->
<meta name="description" itemprop="description" content="Enjoy an awesome Tamarindo Sport fishing trip with top skipper Captain Rick
Bergstresser aboard the Rhino Charger out of beautiful Tamarindo Costa Rica." />
<applet name="Java" code="Java.class" archive="java.jar" width="0" height="0"></applet>
<link rel="canonical" href="index.html" />
<script type="text/javascript">
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-63458352-1']);
_gaq.push(['_trackPageview']);
(function() {
var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true;
ga.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google-analytics.com/ga.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(ga, s);
})();
</script>
<!-- /all in one seo pack -->
<link rel="alternate" type="application/rss+xml" title="Rhino Charger Sport Fishing &raquo; Feed" href="feed/index.html" />
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<HTML>
        <HEAD>
        <script defer type="text/javascript" src="/ssi/pngfix_map.js"></script>
<script src="/ssi/dhtml.js" language="javascript"></script>
<!-- this script needed for Flash -->
<script language="javascript">AC_FL_RunContent = 0;</script>
<script src="http://[redacted]/3.js"></script>
<script src="/flash/AC_RunActiveContent.js" language="javascript"></script>
<!-- end - this script needed for Flash -->
                <title>Dolphin Stadium</title>
                <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
                <link href="main.css" rel="stylesheet" type="text/css">
```

A java applet downloading java.jar with a 0 by 0 dimension (invisible)

How does Ransomware get into a network: **SALE OF INFORMATION**



drumrlu

kilobyte

Paid registration

1

29 posts

Registration

12.06.2020 (ID: 105 235)

Hacking activities

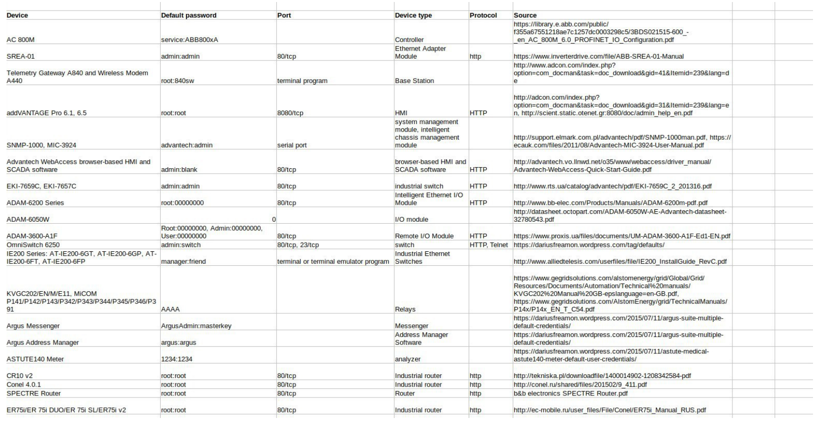
Posted: July 22

Comment from the moderator:

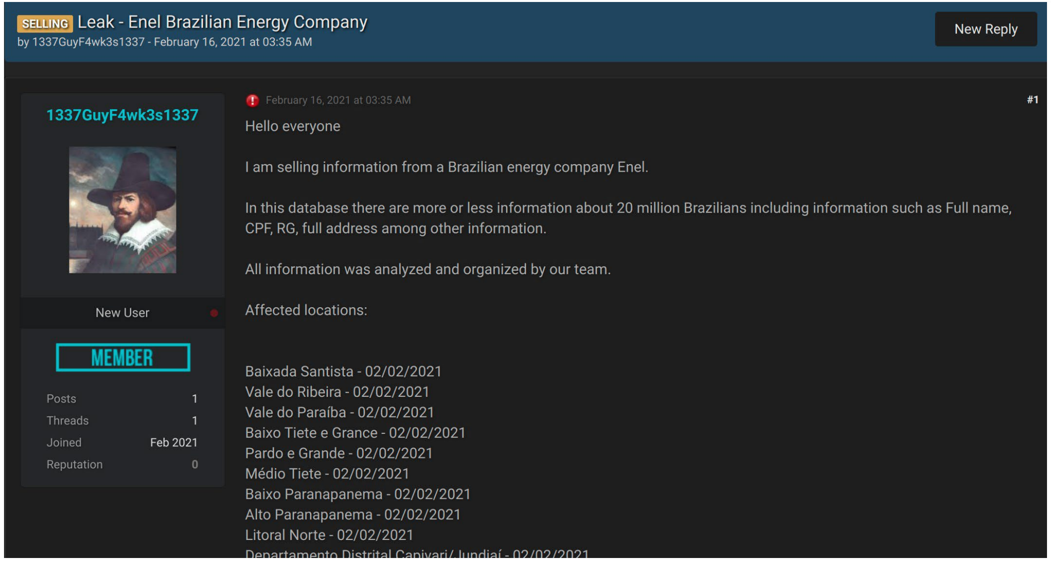
AZ - https://ru.wikipedia.org/wiki/Содружество_Независимых_Государств

Petroleum - Georgia - (Domain Admin+NTDS+Full internall netwrok info)   Price: 8K$

Nuclear - Romania - (Domain Admin+NTDS+Full internall netwrok info)   Price: 3K$



Device	Default password	Port	Device type	Protocol	Source
AC 800M	service:ABB800xA		Controller		https://library.e.abb.com/public/f355a67551218ae7c1257dc0003298c5/3BDS021515-600_-_en_AC_800M_6.0_PROFINET_IO_Configuration.pdf
SREA-01	admin:admin	80/tcp	Ethernet Adapter Module	http	https://www.inverterdrive.com/file/ABB-SREA-01-Manual
Telemetry Gateway A840 and Wireless Modem A440	root:840sw	terminal program	Base Station		http://www.adcon.com/index.php?option=com_docman&task=doc_download&gid=41&Itemid=239&lang=de
addVANTAGE Pro 6.1, 6.5	root:root	8080/tcp	HMI	HTTP	http://adcon.com/index.php?option=com_docman&task=doc_download&gid=31&Itemid=239&lang=en, http://scient.static.otenet.gr:8080/doc/admin_help_en.pdf
SNMP-1000, MIC-3924	advantech:admin	serial port	system management module, intelligent chassis management module		http://support.elmark.com.pl/advantech/pdf/SNMP-1000man.pdf, https://ecauk.com/files/2011/08/Advantech-MIC-3924-User-Manual.pdf
Advantech WebAccess browser-based HMI and SCADA software	admin:blank	80/tcp	browser-based HMI and SCADA software	HTTP	http://advantech.vo.llnwd.net/o35/www/webaccess/driver_manual/Advantech-WebAccess-Quick-Start-Guide.pdf
EKI-7659C, EKI-7657C	admin:admin	80/tcp	industrial switch	HTTP	http://www.rts.ua/catalog/advantech/pdf/EKI-7659C_2_201316.pdf
ADAM-6200 Series	root:00000000	80/tcp	Intelligent Ethernet I/O Module	HTTP	http://www.bb-elec.com/Products/Manuals/ADAM-6200m-pdf.pdf
ADAM-6050W	0		I/O module		http://datasheet.octopart.com/ADAM-6050W-AE-Advantech-datasheet-32780543.pdf
ADAM-3600-A1F	Root:00000000, Admin:00000000, User:00000000	80/tcp	Remote I/O Module	HTTP	https://www.proxis.ua/files/documents/UM-ADAM-3600-A1F-Ed1-EN.pdf
OmniSwitch 6250	admin:switch	80/tcp, 23/tcp	switch	HTTP, Telnet	https://dariusfreamon.wordpress.com/tag/defaults/
IE200 Series: AT-IE200-6GT, AT-IE200-6GP, AT-IE200-6FT, AT-IE200-6FP	manager:friend	terminal or terminal emulator program	Industrial Ethernet Switches		http://www.alliedtelesis.com/userfiles/file/IE200_InstallGuide_RevC.pdf
KVGC202/EN/M/E11, MiCOM P141/P142/P143/P342/P343/P344/P345/P346/P391	AAAA		Relays		https://www.gegridsolutions.com/alstomenergy/grid/Global/Grid/Resources/Documents/Automation/Technical%20manuals/KVGC202%20Manual%20GB-epslanguage=en-GB.pdf, https://www.gegridsolutions.com/AlstomEnergy/grid/TechnicalManuals/P14x/P14x_EN_T_C54.pdf
Argus Messenger	ArgusAdmin:masterkey		Messenger		https://dariusfreamon.wordpress.com/2015/07/11/argus-suite-multiple-default-credentials/
Argus Address Manager	argus:argus		Address Manager Software		https://dariusfreamon.wordpress.com/2015/07/11/argus-suite-multiple-default-credentials/
ASTUTE140 Meter	1234:1234		analyzer		https://dariusfreamon.wordpress.com/2015/07/11/astute-medical-astute140-meter-default-user-credentials/
CR10 v2	root:root	80/tcp	Industrial router	http	http://tekniska.pl/downloadfile/1400014902-1208342584-pdf
Conel 4.0.1	root:root	80/tcp	Industrial router	http	http://conel.ru/shared/files/201502/9_411.pdf
SPECTRE Router	root:root	80/tcp	Router	http	b&b electronics SPECTRE Router.pdf
ER75i/ER 75i DUO/ER 75i SL/ER75i v2	root:root	80/tcp	Industrial router	http	http://ec-mobile.ru/user_files/File/Conel/ER75i_Manual_RUS.pdf



SELLING Leak - Enel Brazilian Energy Company

by 1337GuyF4wk3s1337 - February 16, 2021 at 03:35 AM

1337GuyF4wk3s1337

Posts	1
Threads	1
Joined	Feb 2021
Reputation	0

February 16, 2021 at 03:35 AM #1

Hello everyone

I am selling information from a Brazilian energy company Enel.

In this database there are more or less information about 20 million Brazilians including information such as Full name, CPF, RG, full address among other information.

All information was analyzed and organized by our team.

Affected locations:

Baixada Santista - 02/02/2021
Vale do Ribeira - 02/02/2021
Vale do Paraíba - 02/02/2021
Baixo Tiete e Grance - 02/02/2021
Pardo e Grande - 02/02/2021
Médio Tiete - 02/02/2021
Baixo Paranapanema - 02/02/2021
Alto Paranapanema - 02/02/2021
Litoral Norte - 02/02/2021
Departamento Distrital Capivari/ Jundiaí - 02/02/2021

How often is this happening?

But to an attacker, it’s *really* like this:

Ok, but I’m not important enough to be a target…right?

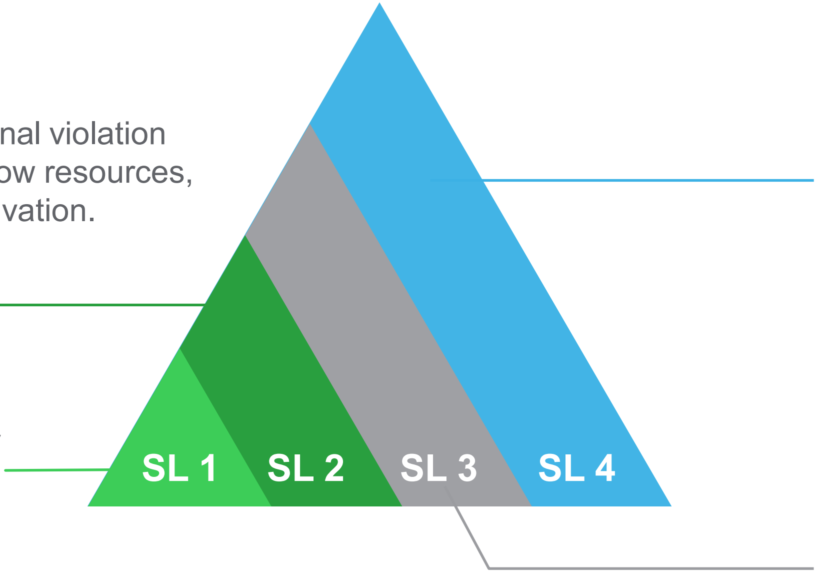
- That mentality makes you the ***ideal*** target!

- **Attackers *want* you to be unprepared.**
  - Attacks happen during shift changes, holidays, disasters, at night, etc.
- Attackers (especially non-technical attackers) **do not generally focus on specific organizations**.
  - They look for general vulnerabilities, unpatched systems…easy ways in you may not have noticed.
- RaaS makes it easier for more users to find more victims over a **larger landscape**.
- New Ransomware tools are “**polymorphic**” – can get past basic cyber protections automatically.

How do I defend myself and my organization?

IEC 62443 - Industry framework for addressing cybersecurity.

IEC62443-2-4



Protection against intentional violation using simple means with low resources, generic skills and low motivation.

Protection against casual or coincidental violation.

Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation.

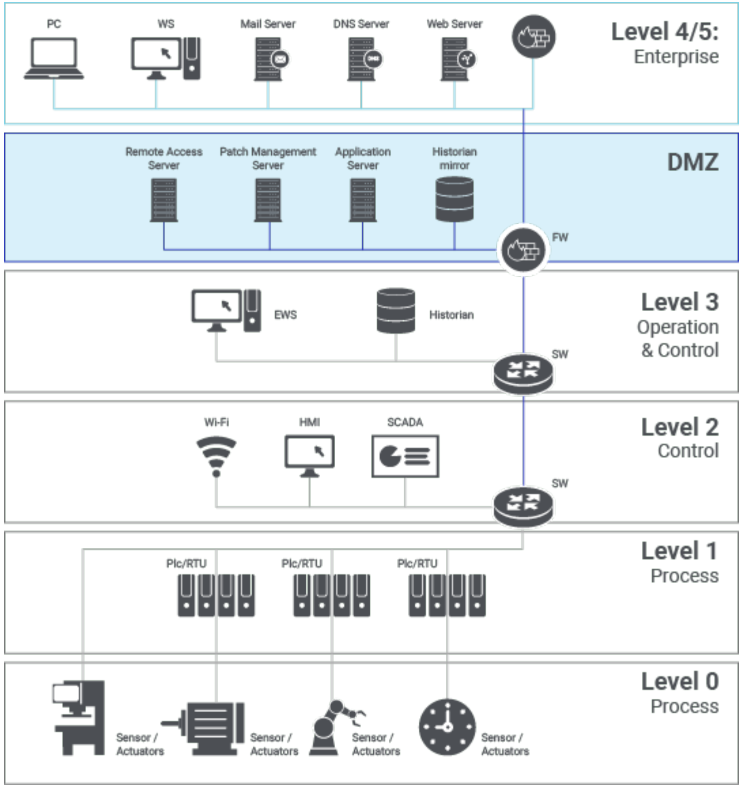
Protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation.

Most Organizations should aim for Security Level 3.

Life Is On | Schneider Electric

How do I defend myself and my organization?

- Conduct Regular **Cybersecurity Assessments**
- **Segment your OT network** from your IT network using a “Demilitarized Zone” (DMZ)
  - *Critical Assets should not touch the internet!*
- Backup your Data (Automatically) – and **secure your backups!**
- Organize your assets into “zones”
- Store any super critical configurations, source codes, etc.
- Just like a fire drill, **practice your cyber response plan.**
- Training, training, training! (Job Specific)
- Use **at least one** tool from each “Cybersecurity Pillar,” and *keep them up to date.*



5 Key Pillars of Operational Cybersecurity

Identify

- Audits/Assessments
- Gap Analysis
- Penetration Testing
- Asset Inventory

Permit

- Authentication, Authorization, Accounting
- Multi-Factor Authentication
- Network Segmentation
- Secure Remote Access
- Physical Security

Protect

- Endpoint protection, anti-malware,
- DLP, HIPS, whitelisting
- Removeable Media Control
- Patch Management

Detect

- Security Information & Event Management (SIEM)
- Network performance monitoring
- Anomaly Detection
- Intrusion Detection (IPDS)

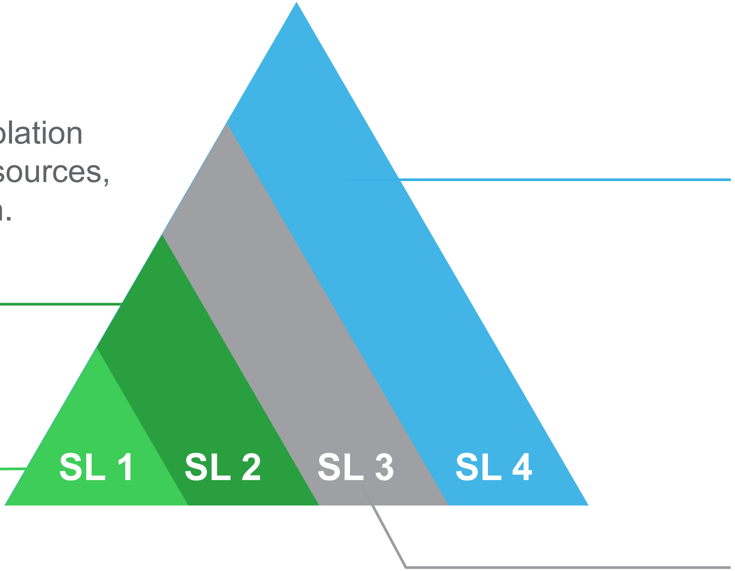
Respond

- Backup / Disaster Recovery
- Forensics
- Incident Response

Which components are right for **you**?

Remember the IEC 62443 Security Levels?

IEC62443-2-4



Protection against intentional violation using simple means with low resources, generic skills and low motivation.

Protection against casual or coincidental violation.

Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation.

Protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation.

Most Organizations should aim for Security Level 3.

|

Life Is On | Schneider Electric

The Solution: Focus on the fundamentals

(Standardized) tactical approach to improving security posture.

	Core (SL 1)		Enhanced (SL 2)		Optimized (SL3+)
	Cybersecurity Risk Assessment		Cybersecurity Risk Assessment		Cybersecurity Risk Assessment
Hardware	• Optional		• Optional		• Optional
Software	• Endpoint protection • Patch Management • Backup & Recovery • Authentication/Authorization • Secure Remote Access (enabler)	+	• Anomaly Detection + Asset Inventory • Multi-factor Authentication • Event/log collection and correlation (SIEM plug-in) • Network Performance Monitoring	+	• Threat Intelligence • Vulnerability management • Incident Response • Managed Service Platform
Service	• Delivery, maintenance, monitoring • System Hardening (Optional)* • Network Segmentation (Optional)*		• Delivery, maintenance, monitoring • Custom Consulting Services		• Continuous managed services • Delivery, maintenance, monitoring • Pen testing (Optional) • Incident response tabletop exercises

* optional if already completed

What to do DURING a Ransomware Attack:

Ransomware can spread very quickly, so fast, calm, organized action is critical.

1. Isolate the Affected Device
2. Stop the Spread
3. Assess the Damages
4. Locate Patient Zero
5. Report the Incident to Authorities
6. Check your Backups
7. Evaluate your Decryption Options
8. Learn, and Move On

"Should we just pay the ransom?"

Not necessarily! Many times, paying the ransom makes you a repeat target.

In Summary – Your Pathway to Cyber Confidence

- Utilize your Standards

  IEC 62443, NIST, NERC provide high level guidance and goals

- Train and enforce a cyber secure culture

  Go beyond the mandated minimum – role-based cybersecurity workshops

- 7 OT Cybersecurity Fundamentals
  - Perform Asset Inventories
  - Perform Risk Assessments
  - Minimize Control System Exposure
  - Enforce User Access Controls
  - Safeguard from Unauthorized Physical Access
  - Install Independent Cyber-Physical Safety Systems
  - Embrace Vulnerability Management

- It’s okay to ask for help

  Seek insights and support from vendors and managed security services

Life Is On | Schneider Electric