ICS Security Survey 2015
Highlights

Over 300 respondents in this year’s SANS ICS Security Survey, with a broad representation of industries.
ICS Survey 2015 - Highlights

Top Three Threat Vectors

- **Internal threat**: 10.6%
- **Integration of IT into control system networks**: 19.4%
- **External threats (hacktivism, nation states)**: 42.1%
Known Breaches in past 12 months

- **Unknown/Unable to answer**
  - 2015: 40.0%
  - 2014: 35.0%

- **26 +**
  - 2015: 3.0%
  - 2014: 2.0%

- **11 to 25**
  - 2015: 5.0%
  - 2014: 6.0%

- **6 to 10**
  - 2015: 15.0%
  - 2014: 15.0%

- **3 to 5**
  - 2015: 20.0%
  - 2014: 25.0%

- **1 to 2**
  - 2015: 30.0%
  - 2014: 30.0%
How high is the current cybersecurity threat to control systems?

- **Low**:
  - Decision Influencers Perception of Current Threat: 0.0%
  - Decision Makers Perception of Current Threat: 15.0%

- **Moderate**:
  - Decision Influencers Perception of Current Threat: 5.0%
  - Decision Makers Perception of Current Threat: 35.0%

- **High**:
  - Decision Influencers Perception of Current Threat: 10.0%
  - Decision Makers Perception of Current Threat: 40.0%

- **Severe**:
  - Decision Influencers Perception of Current Threat: 10.0%
  - Decision Makers Perception of Current Threat: 0.0%
Mapping of Control System Security to Cybersecurity Standards

- NIST Guide to SCADA and Industrial Control Systems Security
- NERC CIP
- Critical Security Controls
- ISA99 (Industrial Automation and Control Systems Security)/IEC 62443
- ISO 27000 series including 27001 and others
- Other
- ENISA Guide to Protecting ICS—Recommendations for Europe and Member States
- ISA100.15 Backhaul Network Architecture
- Qatar ICS Security Standard
- Chemical Facility Antiterrorism Standards (CFATS)
Does your company have a security strategy to address the convergence of information and operational technologies?

- 35.6%: We have a strategy and are implementing it.
- 29.4%: We have a strategy in place.
- 17.5%: We have no strategy nor plans to develop one.
- 17.5%: We have no strategy but are developing one.
ICS Survey 2015 – Highlights

Top Control System Security Initiatives

- Perform security assessment/audit: 17.2%
- Increased security awareness training: 15.5%
- Increased physical security: 13.3%
- Increased security staffing: 9.9%
- Increased security training: 9.0%
- Implement intrusion detection tools: 8.2%
- Implement intrusion prevention tools: 6.4%
- Increased security consulting services: 6.0%
- Implement anomaly detection tools: 6.0%
- Increased background security checks: 3.4%
- Greater mobile devices/wireless communications controls: 2.6%

Graphical representation of the above data.
The State of Security in Control Systems Today: A SANS Survey Webcast:

Twitter: 
@SANSICS

SANS ICS Blog: 
http://ics.sans.org/blog

LinkedIn: 
https://www.linkedin.com/company/sans-ics
EXTRA SLIDES
Which control system components do you consider at greatest risk for compromise

- Computer assets running commercial OS
- Connections to other internal networks
- Networking devices
- Control system communication protocols
- Field SCADA network connections
- Wireless communication devices and protocols
- Embedded controllers and other components
- Control system applications
- Other
- Physical access systems
- Plant historian
- OLE for process control (OPC)
Time from initial attack to ICS security staff awareness of incident

- Unknown: 20%
- Immediately: 7%
- <=1 hour: 19%
- 1–24 hours: 15%
- 1–7 days: 19%
- 8–30 days: 6%
- >30 days: 15%
When did your organization most recently perform a security assessment of your control systems or control system networks?

- 52.0% within the past 6 months
- 22.6% in the past 7–12 months
- 8.5% in the past 13–24 months
- 8.5% more than 24 months ago
- 8.5% never

ICS Survey 2015 – Highlights