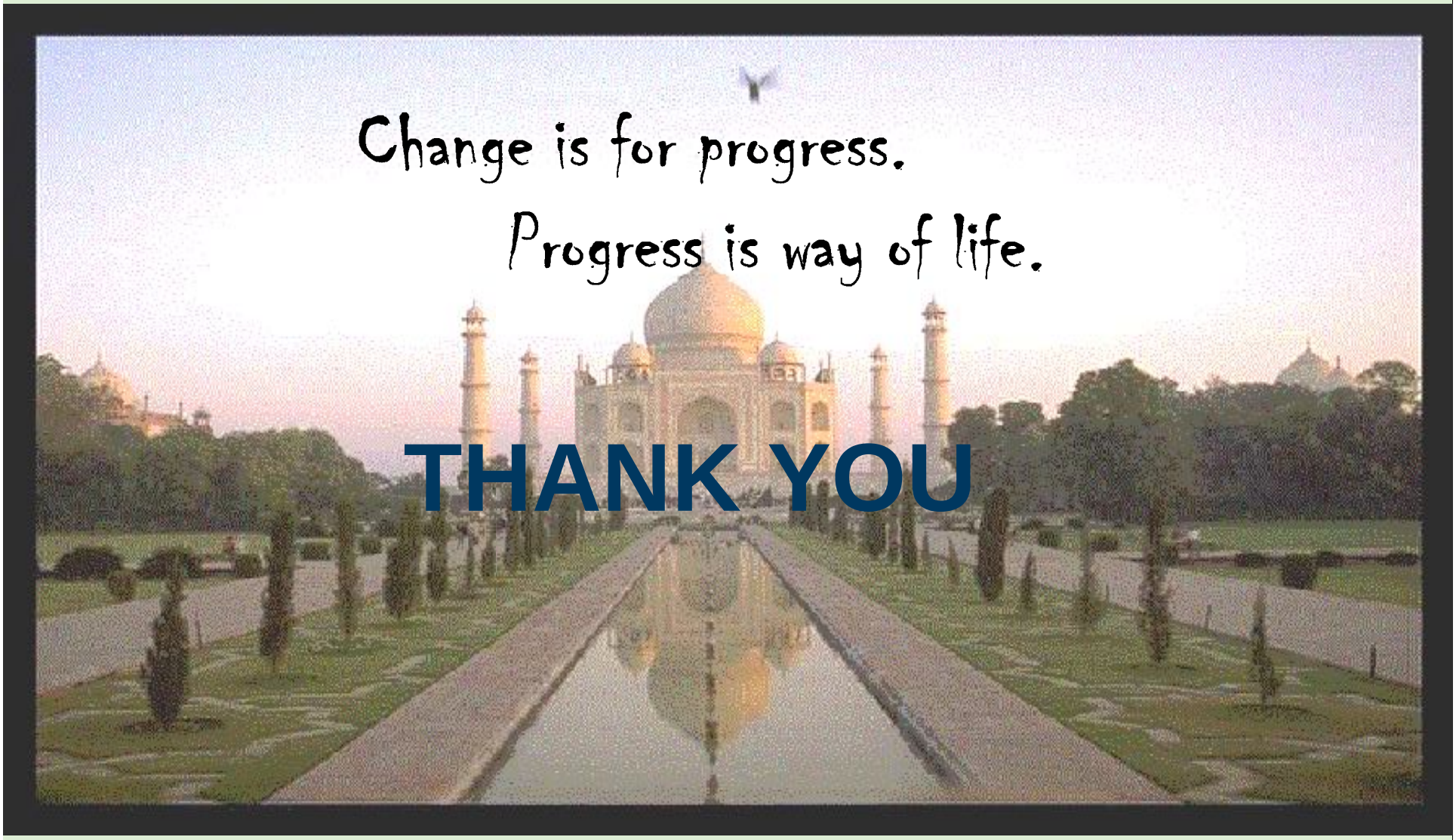
INSTT & AUTOMATION – KEY ENABLER

- **An Integrated End to End solution from production to distribution**
- **Unified automation platform for process controls, safety and optimization solutions with latest IT tools**
- **User friendly interface systems and plant wide data transfer**
- **Flexibility to incorporate customized solutions**
- **Seamless data exchange from production to distribution and conversion of historical data to information for analysis, mitigation actions and management decisions**
- **Implementation of management information system functions**
- **Reduction in plant downtime with predictive and preventive maintenance of equipments through asset management system**

INSTT & AUTOMATION – OPPORTUNITIES

- VFDs use in electrical drives for energy conservation
- Control of Fired Heater operations for safety and energy efficiency
- Process integration for operating at optimum parameters
- Advance Process Control for reducing product give – aways
- Increased recycling for enhancing product yield / energy efficiency
- Dryer / PSA bed operation / regeneration cycle automation
- Safe Burner Management System by sequencing of interlocks
- CW system on-line monitoring and control for chemical treatment
- Flare load minimisation through instt / automation

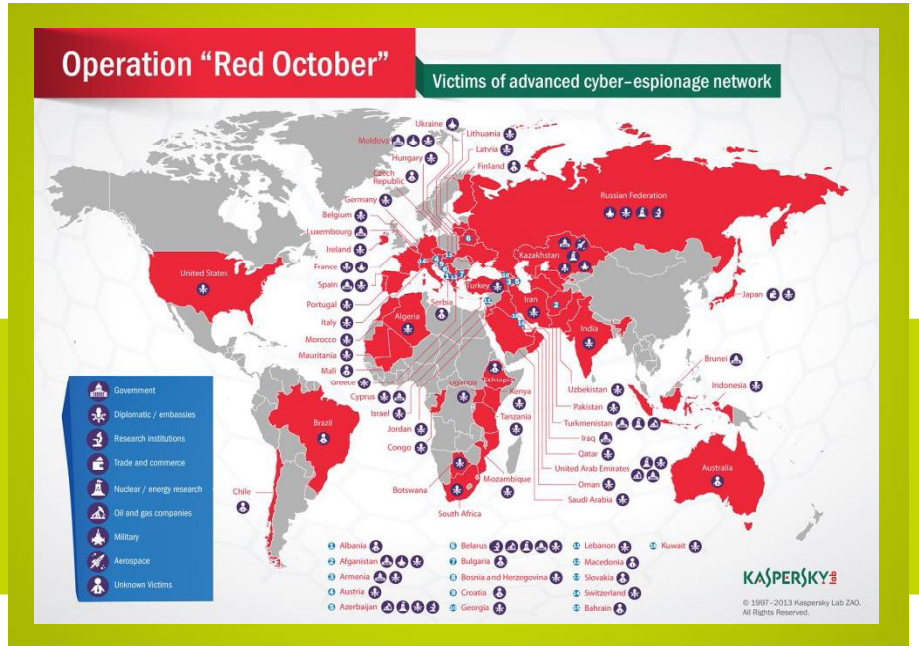
Instrumentation



TM

Invensys Cyber Security Services

Protecting Plant Assets With Cyber Security



Glen Bounds

Global Modernization Consultant

Invensys Cyber Security Services

invensys

Agenda

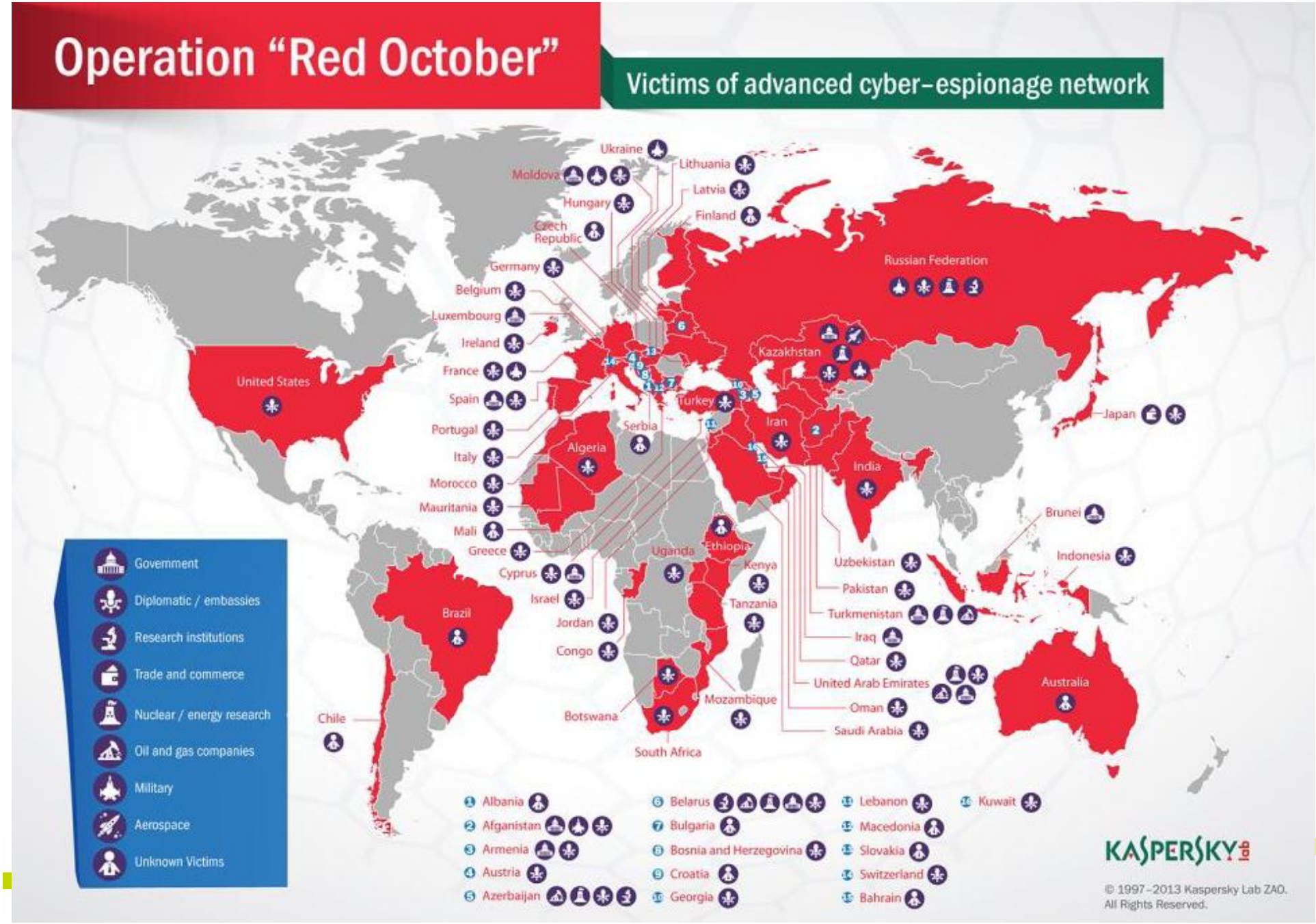
Cyber Security Defined

Recommended Solutions

Summary

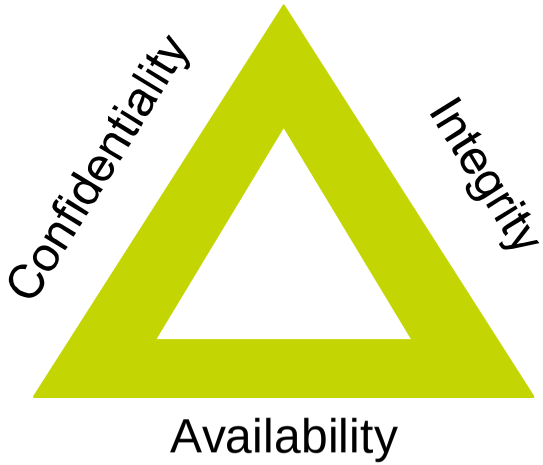
Cyber Security Defined

invensys™


Operation "Red October"
Victims of advanced cyber-espionage network
Ukraine
Moldova
Lithuania
Latvia
Hungary
Finland
Czech Republic
Germany
Belgium
Luxembourg
Ireland
France
Spain
Portugal
Italy
Morocco
Mauritania
Mali
Greece
Cyprus
Israel
Jordan
Congo
Chile
Brazil
United States
Russian Federation
Kazakhstan
Turkey
Serbia
Algeria
Iran
India
Japan
Brunei
Indonesia
Uzbekistan
Pakistan
Turkmenistan
Iraq
Qatar
United Arab Emirates
Oman
Saudi Arabia
Australia
Uganda
Ethiopia
Kenya
Tanzania
Mozambique
Botswana
South Africa
Government
Diplomatic / embassies
Research institutions
Trade and commerce
Nuclear / energy research
Oil and gas companies
Military
Aerospace
Unknown Victims
1 Albania
2 Afganistan
3 Armenia
4 Austria
5 Azerbaijan
6 Belarus
7 Bulgaria
8 Bosnia and Herzegovina
9 Croatia
10 Georgia
11 Lebanon
12 Macedonia
13 Slovakia
14 Switzerland
15 Bahrain
16 Kuwait
KASPERSKY lab
© 1997-2013 Kaspersky Lab ZAO.
All Rights Reserved.

Priorities for Cyber Security

Traditional IT

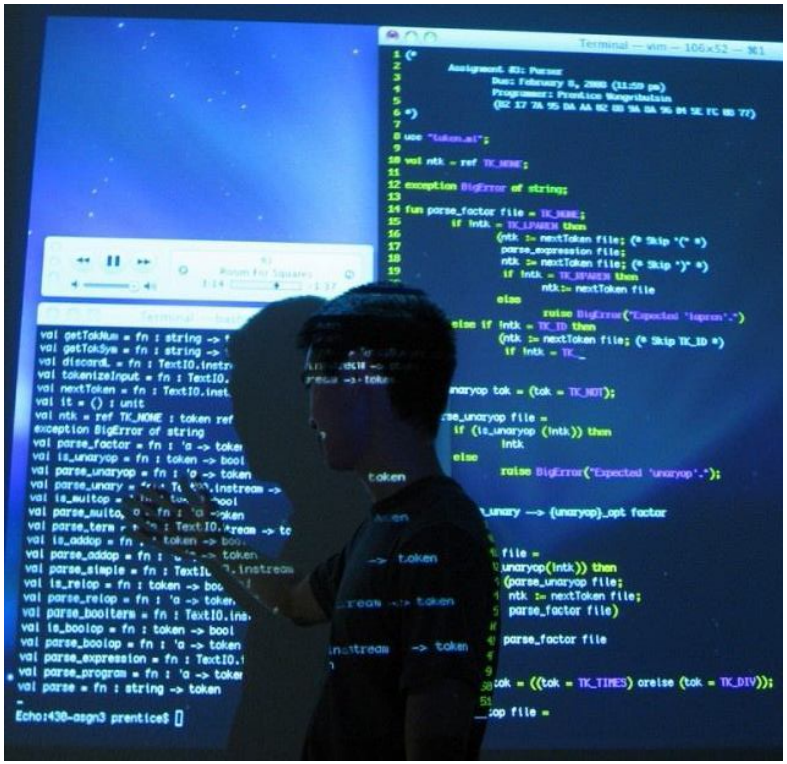


Automation

invensys™

ICS Cyber Security Defined

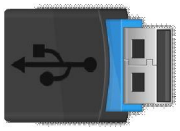
The ability to control and prevent unauthorized external or internal access to critical infrastructure systems



- **Why it's important**
  - Increases (plant) safety
  - Reduces down time
  - Protection of intellectual property
  - Compliance with internal regulations
  - Compliance with country-specific regulations

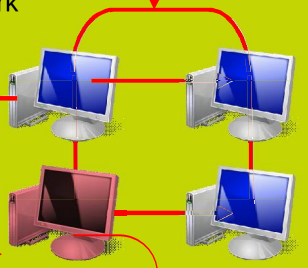
How a Virus can cripple a Nation

The virus is placed on a USB Drive

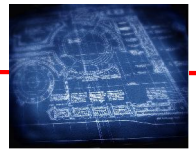


Enters a secure internal Network

The virus scans through the network



It takes a blueprint of the network and relays it to an external server



A new updated virus targets specific computers

It sends back false messages that the machines are fine

It tells the machines to damage or destroy themselves

It subverts the computers running specific machines

The virus subverts the software controlling entire industrial operations

CRITICAL INFRASTRUCTURE COMPROMISED

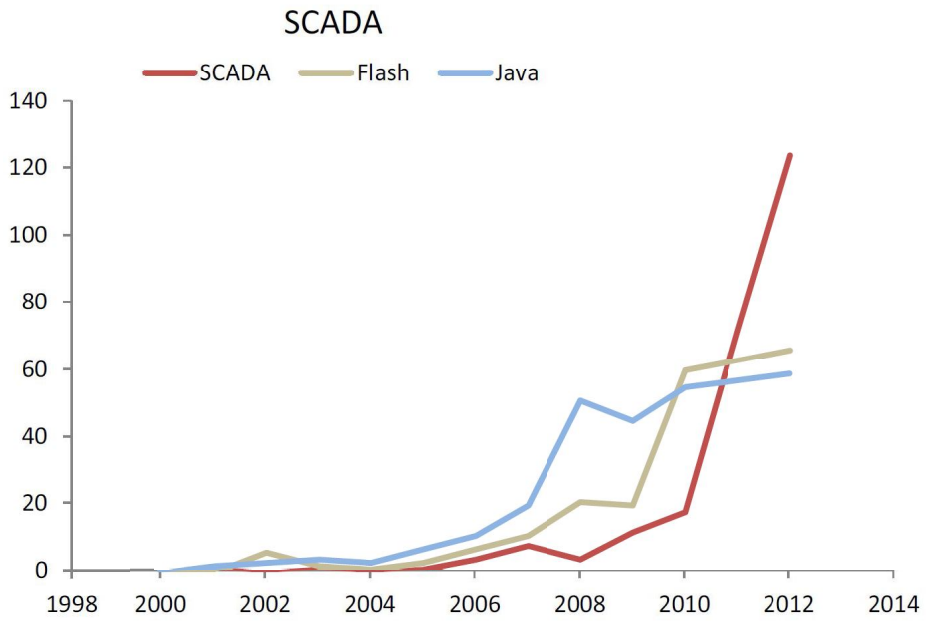
The virus spreads to other, highly interconnected infrastructures

- Power Plants
- Oil & Gas Refineries
- Sewage Treatment
- Transport

REGIONAL AND NATIONAL INFRASTRUCTURES COLLAPSE

invensys™

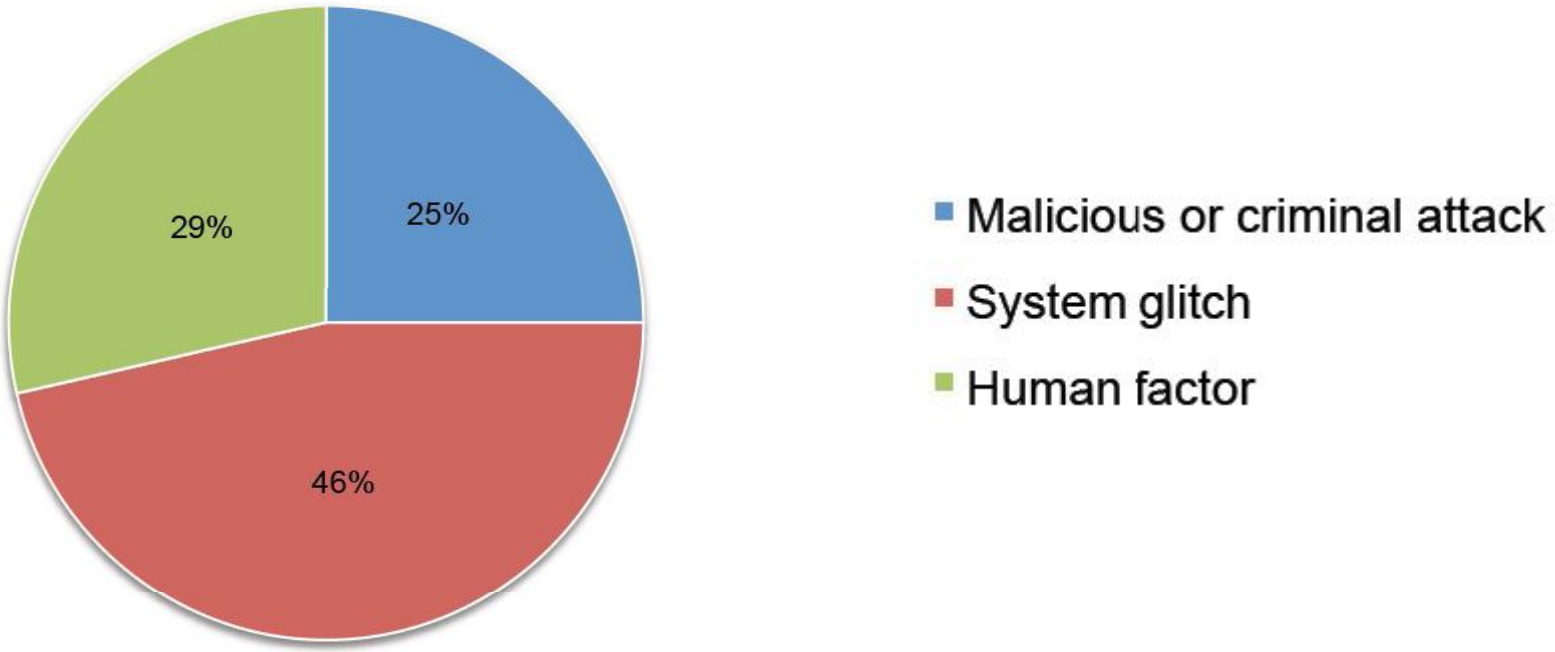
Recent Headlines:
The Threats are Real



NSS Labs Vulnerability Report - 2013

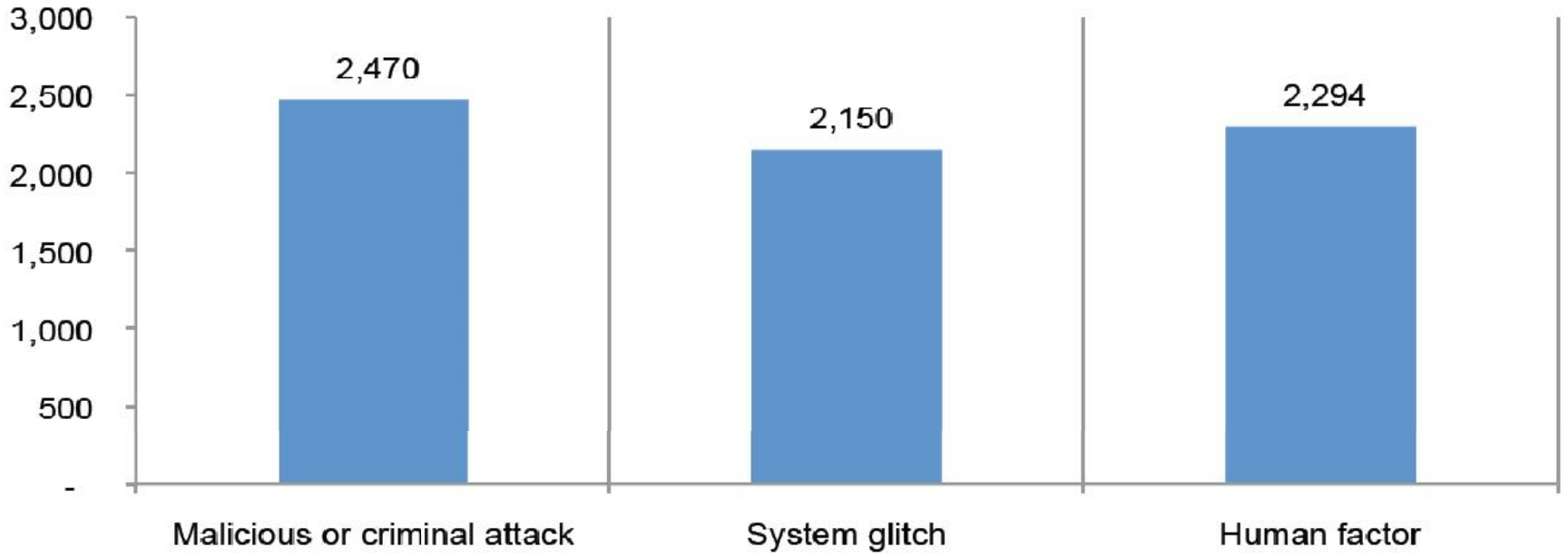
- ICS/SCADA vulnerabilities have increased more than 600% since 2010
- Cyber-Espionage / Malware programs steal sensitive data from organizations for 5 YEARS before being discovered
- Power companies targeted by approximately 10,000 cyber attacks per month
- Hackers target proprietary ICS, PLC, and SCADA technologies

Distribution of the benchmark sample by root cause of the data breach



Ponemon Institute© Research Report - *2012*

Per capita cost for three root causes of the data breach - Measured in INR



Ponemon Institute© Research Report - *2012*

Recent Occurrences:

Attacks on National Critical Infrastructure

Actual Code Extracts - Stuxnet Virus

Stuxnet Facts:

- Discovered June, 2010
- Targeted to attack Iran's nuclear facilities
- Spread via Microsoft Windows
- Created for a specific Industrial Control SCADA System
- Initially spread via USB, then Peer to Peer
- Designed to force a change in the centrifuge's rotor speed

Recent Occurrences:

Attacks on National Critical Infrastructure

Actual Code Extracts - Shamoon Virus

Shamoon Facts:

- Discovered August, 2012
- Targeted to attack Saudi & Qatar-Based Energy Companies
- Spread via Microsoft Windows
- Destroyed Master Boot Record of 42,000 systems
- Initially spread via USB, then Peer to Peer
- Designed to cause disruption only

Recent Occurrences:

Attacks on National Critical Infrastructure

```
if ( SystemTime.wYear >= var_loc_target_time.wYear )
{
  if ( SystemTime.wMonth >= var_loc_target_time.wMonth
    && SystemTime.wDay >= var_loc_target_time.wDay
    && SystemTime.wHour >= var_loc_target_hour
    && SystemTime.wMinute >= var_loc_target_minute )
    var_loc_before_target_date = 0;
  if ( SystemTime.wYear == var_loc_target_time.wYear )
  {
    if ( SystemTime.wMonth == var_loc_target_time.wMonth )
    {
      if ( SystemTime.wDay == var_loc_target_time.wDay )
      {
        if ( SystemTime.wHour == var_loc_target_hour )
        {
          v3 = var_loc_target_minute - SystemTime.wMinute;
          if ( v3 < 2 )
          {
            var_loc_before_target_date = var_loc_target_mir
            if ( v3 < 0 )
              var_loc_before_target_date = 0;
          }
        }
      }
    }
  }
}
```

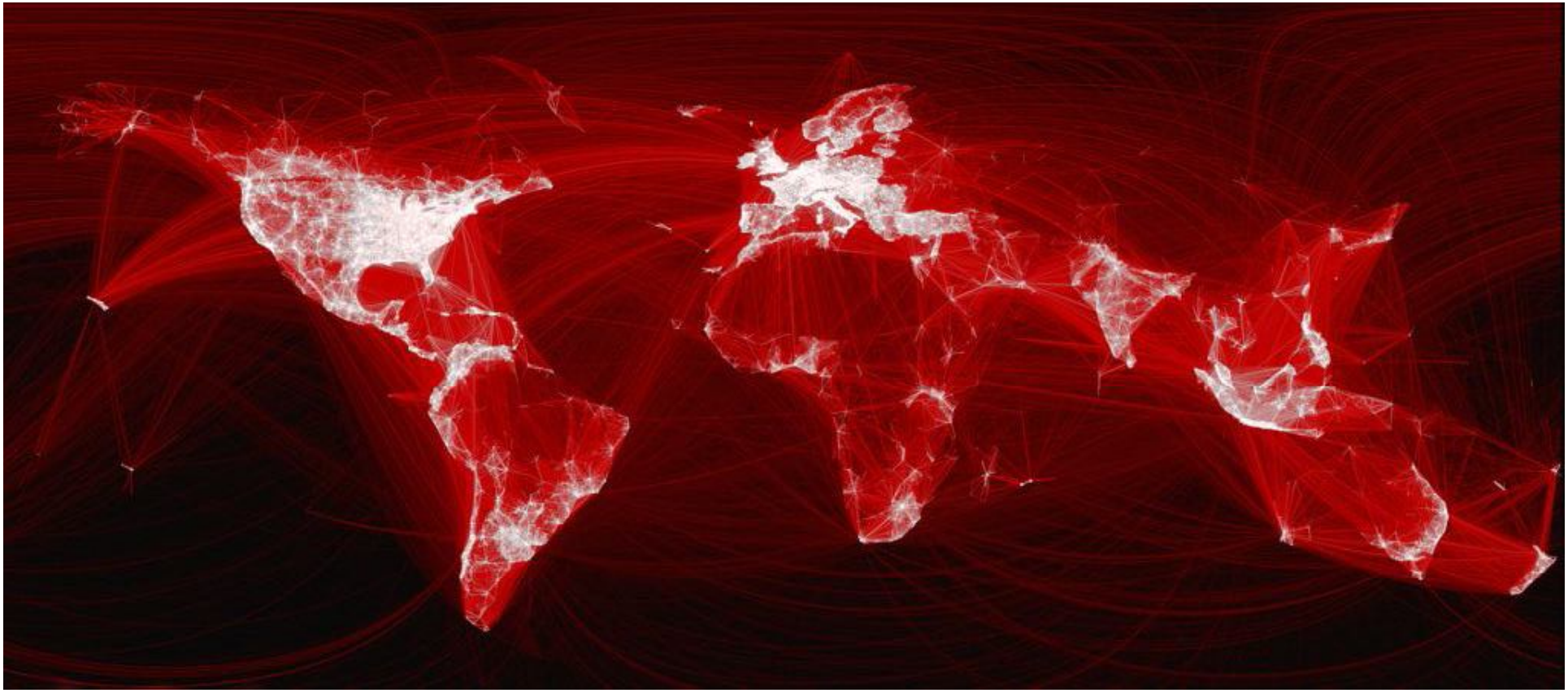
```
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul | findstr -i download 2>nul
>f1.inf
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul | findstr -i document 2>nul
>>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul | findstr -i download 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul | findstr -i document 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul | findstr -i picture 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul | findstr -i video 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul | findstr -i music 2>nul >>f1.inf
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul | findstr -i desktop 2>nul
>f2.inf
dir C:\Users\ /s /b /a:-D 2>nul | findstr -i desktop 2>nul >>f2.inf
dir C:\Windows\System32\Drivers /s /b /a:-D 2>nul >>f2.inf
dir C:\Windows\System32\Config /s /b /a:-D 2>nul | findstr -v -i systemprofile
2>nul >>f2.inf
dir f1.inf /s /b 2>nul >>f1.inf
dir f2.inf /s /b 2>nul >>f1.inf
```

Recent Occurrences:

Attacks on National Critical Infrastructure

```
typedef struct {
        HMODULE Handle_NtdllDll;
        DWORD field_4;
        int (__stdcall *proc_lstrcmpiW)(LPCTSTR lpString1, LPCTSTR lpString2);
        SIZE_T (__stdcall *proc_VirtualQuery)(LPCVOID lpAddress, PMEMORY_BASIC_INFORMATION lpBuffer, SIZE_T dwLength);
        BOOL (__stdcall *proc_VirtualProtect)(LPVOID lpAddress, SIZE_T dwSize, DWORD flNewProtect, PDWORD lpflOldProtect);
        FARPROC (__stdcall *proc_GetProcAddress)(HMODULE hModule, LPCSTR lpProcName);
        LPVOID (__stdcall *proc_MapViewOfFile)(HANDLE hFileMappingObject, DWORD dwDesiredAccess, DWORD dwFileOffsetHigh,
        DWORD dwFileOffsetLow, SIZE_T dwNumberOfBytesToMap);
        BOOL (__stdcall *proc_UnmapViewOfFile)(LPCVOID lpBaseAddress);
        BOOL (__stdcall *proc_FlushInstructionCache)(HANDLE hProcess, LPCVOID lpBaseAddress, SIZE_T dwSize);
        HMODULE (__stdcall *proc_LoadLibraryW)(LPCTSTR lpFileName);
        BOOL (__stdcall *proc_FreeLibrary)(HMODULE hModule);
        NTSTATUS (__stdcall *proc_ZwCreateSection)(PHANDLE SectionHandle, ACCESS_MASK DesiredAccess, DWORD ObjectAttributes,
        PLARGE_INTEGER MaximumSize, ULONG SectionPageProtection, ULONG AllocationAttributes, HANDLE FileHandle);
        NTSTATUS (__stdcall *proc_ZwMapViewOfSection)(HANDLE SectionHandle, HANDLE ProcessHandle, PVOID *BaseAddress,
        ULONG_PTR ZeroBits, SIZE_T CommitSize, PLARGE_INTEGER SectionOffset, PSIZE_T ViewSize, DWORD InheritDisposition,
        ULONG AllocationType, ULONG Win32Protect);
        HANDLE (__stdcall *proc_CreateThread)(LPSECURITY_ATTRIBUTES lpThreadAttributes, SIZE_T dwStackSize,
        LPTHREAD_START_ROUTINE lpStartAddress, LPVOID lpParameter, DWORD dwCreationFlags, LPDWORD lpThreadId);
        DWORD (__stdcall *proc_WaitForSingleObject)(HANDLE hHandle, DWORD dwMilliseconds);
        BOOL (__stdcall *proc_GetExitCodeThread)(HANDLE hThread, LPDWORD lpExitCode);
        NTSTATUS (__stdcall *proc_ZwClose)(HANDLE Handle);
} obfuscatedImports;
```

invensys™



FACT

What do we do?

Flawless operation of critical infrastructure

A Primary Component of National Security

invensys™

Agenda

Cyber Security Defined

Recommended Solutions

Summary

Recommended Solutions

invensys™

Standards and Best Practices:

IEC 62443-3-3 (ISA99) Foundation Requirements:

- Identification and authentication control
- Use control
- System integrity
- Data confidentiality
- Restricted data flow
- Timely response to events
- Resource availability

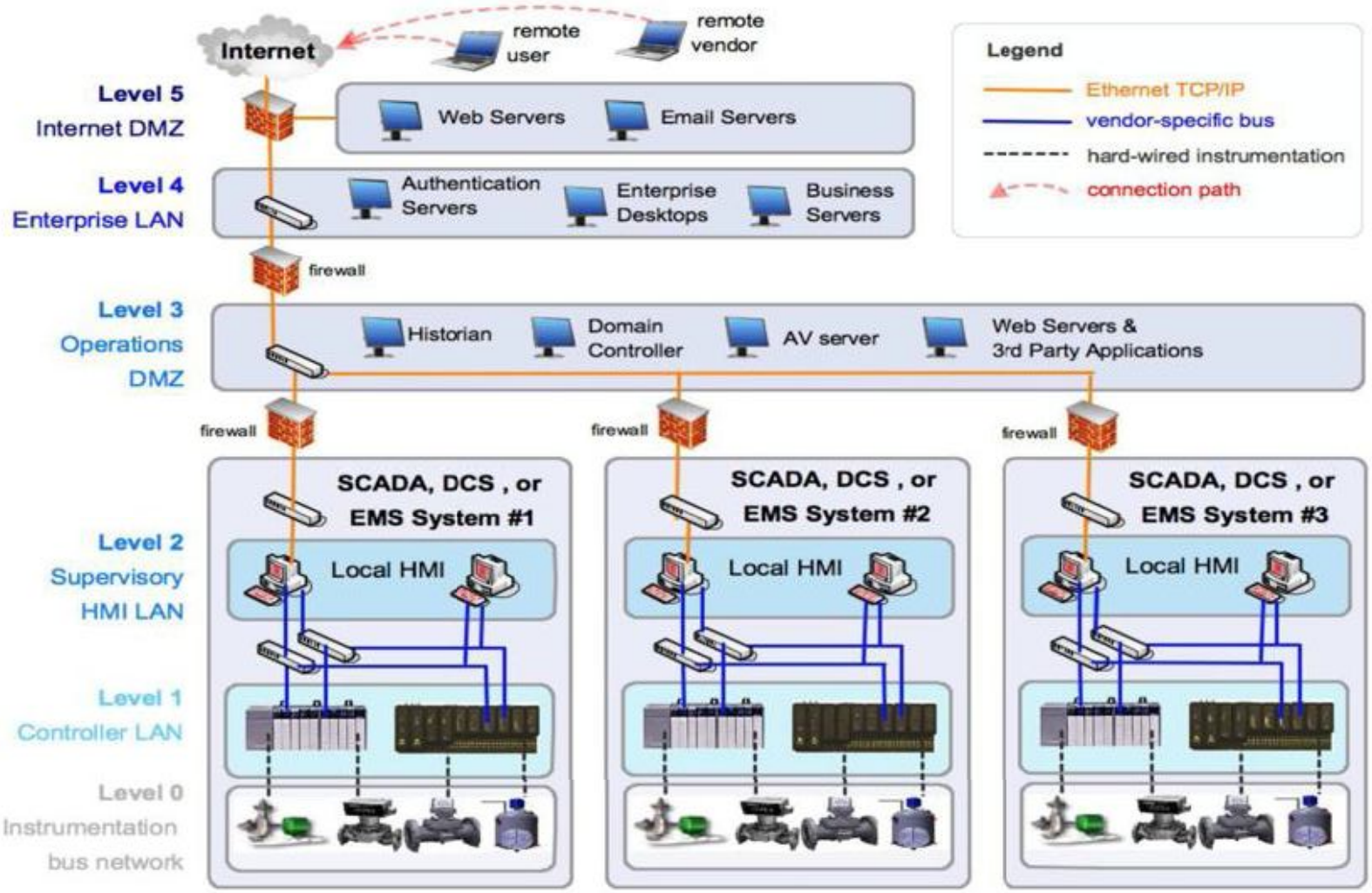
- Hacker's definition of Standards:
- A box to play in….

ISO 27001

NERC - North American Electric Reliability Corporation

NIST - National Institute of Standards and Technology

Industrial Network Overview



Industrial Network Security Challenges

Increased Complexity and Connectivity

- Corporate Access, Remote Access Wireless, PCs, TCP/IP

Evolving Threat Landscape

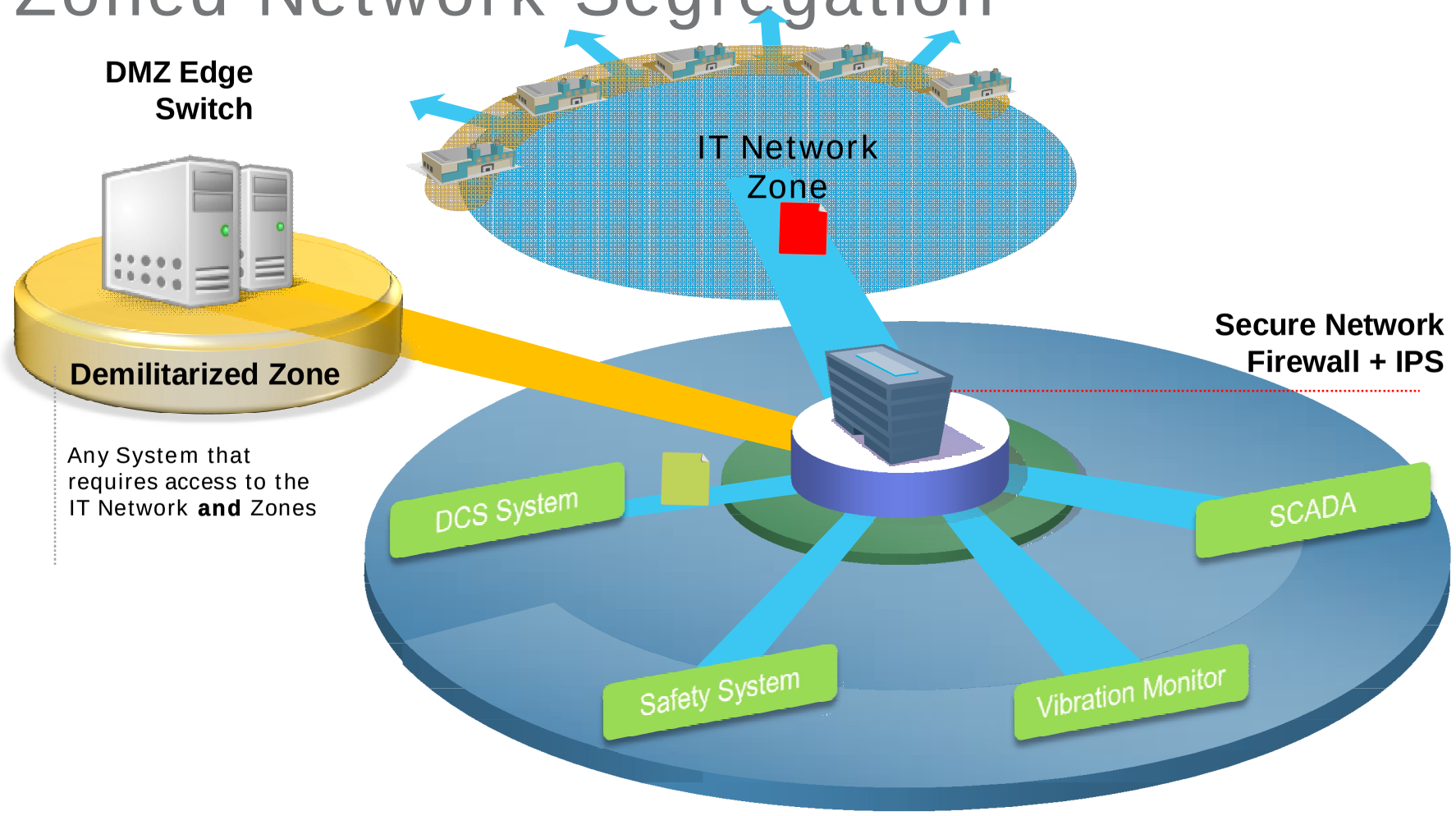
- Advanced Persistent Threat Attacks (APT)
  - Stuxnet, Duqu, Flame, Gauss, Shamoon, ???
  - Malware (Drive-by Exploits)
  - Cloud-based Solutions
  - Insider Threat
  - Social Engineering

Recommended Cyber Security Solutions

- **Role Based Access Controls / Centralized Management**
- **Complete Endpoint Protection**
- **Ethernet Switch Hardening**
- **Complete System Monitoring & Management**
- **Disaster Recovery**
- **Implementation of BIOS Security**

DL380 BIOS Parameters	Setting
System Options > USB Options > Removable Flash Media Boot Sequence	Internal SD Card First
System Options > Processor Options > No-Execute Memory Protection	Enabled
Standard Boot Order (IPL)	Reordered 1. Hard Drive C: 2. CD-ROM 3. Floppy Drive 4. USB DriveKey 5. PCI Slot 5 Ethernet Network Controller 6. PCI Slot 6 Ethernet Network Controller
Server Availability > POST F1 Prompt	Delayed (20 Seconds)
Server Security > Set Admin Password	Set to a strong password that will be communicated only to authorized users
BIOS Serial Console & EMS > BIOS Serial Console Port	Disabled

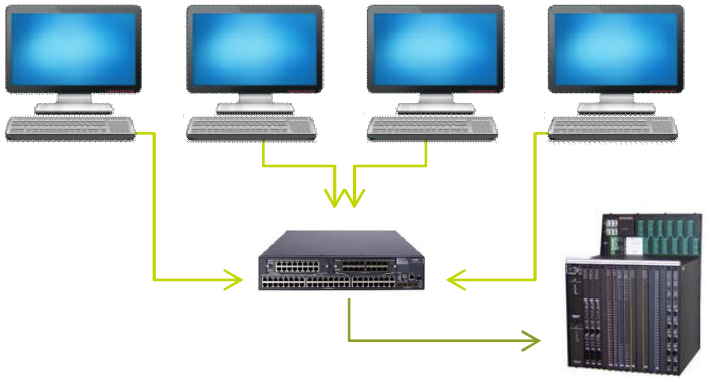
Second Ethernet with Zoned Network Segregation



Security-Enhanced Solutions

Isolated Systems

Networked Systems



Microsoft Windows Active Directory

- Centralized system management
- Individual User logons
- Group-based security policies

Microsoft Patch Management

- Centralized distribution

Centralized Endpoint Protection

- Host Intrusion Prevention
- Anti Virus / Anti Spyware
- Device Management (DLP)

Centralized Backup

- Disaster recovery
- System restoration

Network Segmentation

- Network-based AV / AS
- Network-based IPS
- Strict access policies

Centralized monitoring

- System Management
- System Availability
- Alerting and reporting

Preventative Security Maintenance

- **Vulnerability assessments**
- **Network and system audits**
- **Network and system hardening**
- **Infrastructure evaluations**
- **Security program review / development**
- **Information security training**
- **Disaster Recovery / Business continuity**

29AVSR01 – W2K3 Anti Virus Server		
TASK	**PRIOR State**	**POST State**
Vulnerability level		
Insecure open ports	TCP 139 NETBIOS TCP 3389 RDP TCP 21 FTP UDP 5004 RTP UDP 445 MS SMB File Sharing	Closed via FW Policy Managed via FW Policy Closed via FW Policy Required for EPO Required for AV Updates
Insecure running services	Internet Information Service FTP Server Service Terminal Services	Required for EPO Closed via FW Policy **If not required, disable**
AV client	McAfee 8.7	Unchanged
AV DEFs	April 2 2011	December 9 2011
AV auto update	None	Unchanged (AV Srvr Manual)
AV scheduled scan	None	Yes / Monthly / Day 1 / 1AM
AV Scans run recently	None	Yes – Clean
AV buffer overflow protection	Enabled	Unchanged
Operating System patches	Up until 6/2008	See page 14
Security and system logging	Yes / Local / 512KB / 7 days	Yes / Local / 1024KB / 90 days
Complex Admin password	None	SPDIAManager / PW
Decoy Admin account	None	Decoy admin account created
Default accounts	In use	Disabled
Games	Not installed	Unchanged
Internet Services	Installed	Required
Language compilers	Not installed	Unchanged
Unused network components	Not installed	Unchanged
Unused configuration files	Located on C and D roots	Deleted
Backup methodology	Symantec BESR 8 / Monthly / Day 2 / 7PM	Changed to only keep 2 versions of each backup. See page 18.
Other / Notes	EPO Agents not communicating / No agent tasks / No scan tasks	EPO Agent reinstalled, communicating successfully / Update tasks created via Agent / Scan tasks added

invensys™

Monitor

How can you know if your assets are protected if you don’t monitor the data?

Agenda

- Cyber Security Defined
- Recommended Solutions
- **Summary**

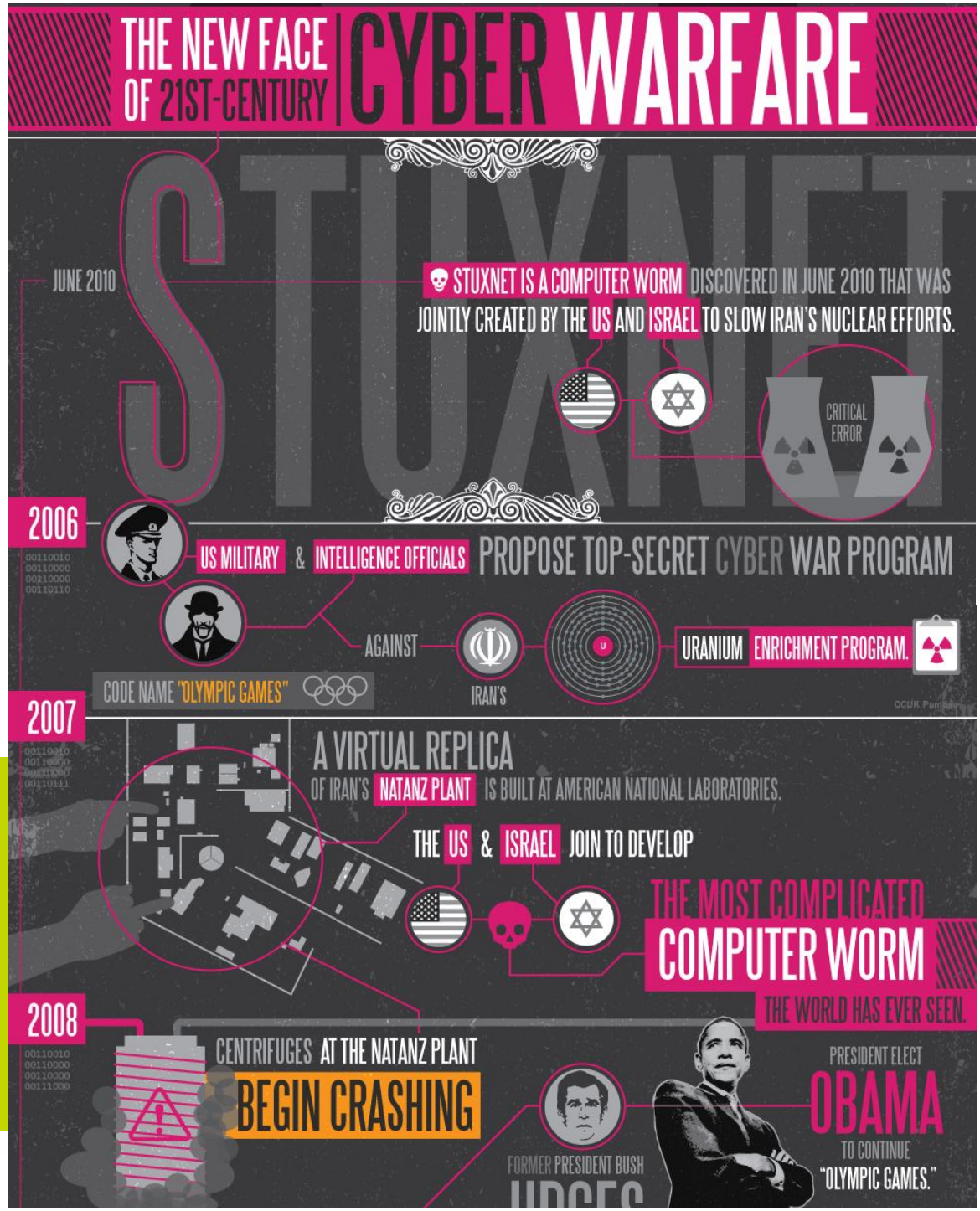
Summary

invensys™

1. Creating and maintaining a Cyber Security plan is absolutely critical.
2. Plan must be approved and supported by Executive Management.
3. Plan must include a Business Continuity strategy.
4. Security must be designed into the initial stages of Operating Platform development.

"Safety and Cyber Security are job one at Invensys"

Mike Caliel - President & CEO
Invensys Operations Management



THANK YOU

Glen Bounds

Global Modernization Consultant

Glen.bounds@invensys.com

Cyber Security

Avantis Eurotherm Foxboro IMServ InFusion SimSci-Esscor Skelta Triconex Wonderware

invensys™
Operations Management

Selection of Switching Interface – A Need for Reliable Control Systems

ISA

finder
The power in relays