Cambridge Centre for Risk Studies

The Future of Cyber Risk

Conference July 2019

The Future of Cyber Risk

Dr. Andrew Coburn Chief Scientist Cambridge Centre for Risk Studies

Centre for **Risk Studies**





Cambridge Center for Risk Studies: Taxonomy of Business Risks



Flood

Financial

Shock

Catastrophe

Outbreak

Disease

Volcanic

Eruption

Waterborne

Epidemic

Natural















Humanitarian

Crisis

Child

Poverty



Dispute

Catastrophe

Hail

Trade





















Plant Epidemic







Electric Heatwave Storm











Welfare Refugee Failure Crisis







Wildfire Pollution Event









Externality

Space

Threat





Meteorite

Solar Storm

Conventional War

Asymmetric War

Nuclear

Sea Level Rise

Ocean System Change

War







Industrial Accident

Technological Catastrophe







Cyber



Technological Infrastructure Accident Catastrophe

Failure





Cambridge Center for Risk Studies: Taxonomy of Business Risks









Financial

Natural

Disease

xternality

Cyber as a Systemic Risk



- In 2012 identified the potential for cyber to pose a systemic risk
- 'Systemically Important Technology Enterprises' (SITEs)
 - Industry standard software platforms providing common failure pathways
- Key issue for managing accumulation risk in cyber insurance portfolios





NotPetya A Real World Example of Systemic Cyber Risk



- 27 June 2017, contagious malware attack caused \$10 Bn loss
- Over 2,000 infections in organizations across 65 countries
- Hidden in the software update mechanism of M.E.Doc (uk), Ukrainian tax filing program





Nodes of Aggregation: Organization Attack Surface

| 12 Principal Classes | | 32 Sub-Classes | | | Primary Vendors | | | Products | |
|----------------------|----------------------------|----------------|------------------------|---|-----------------------|-------------------|--------------|-------------------|--|
| А | Compute | | | | above 1% market share | | | | |
| В | Storage | | | | | | | Versions | |
| С | Network Security | C.1 | Firewall | | | | | Tens of thousands | |
| D | Network & Content Delivery | C.2 | Antivirus | | | | Market share | | |
| Е | Database | C.3 | Email Service Security | | C.3.1 | Apple iPhone | | | |
| F | Cloud Operations | C.4 | ISP | , | C.3.2 | Gmail | | | |
| G | Financial Systems | | | | C.3.3 | Apple iPad | | | |
| Н | Customer Engagement | | | | C.3.4 | Apple Mail | | | |
| I | E-Commerce Platform | | | | C.3.5 | Outlook | | | |
| J | Industrial Systems | | | | C.3.6 | Samsung | | | |
| K | Mobile Services | | | | C.3.7 | Google Android | | | |
| L | Human Capital Management | | | | C.3.8 | Outlook.com | | | |
| | | | | | C.3.9 | Yahoo! Mail | | | |
| | | | | | C.3.10 | Windows Live Mail | | | |
| | | | | | | | | | |

0% 10% 20% 30% 40%



An Extensive Programme of Cyber Risk Research



2013 Cyber Catastrophe Threat Monograph



2018 Threat Actors in the Cyber Black Economy



Sybil Logic Bomb Stress Test Scenario



2018 Assessing Limits to Capabilities of rDDoS Cyber Attacks



Business Blackout CNI Scenario



2018 Insights from the MISP Database



2016 Exposure Data Schema and Accumulation Risk







2018 Cloud Outage: The Potential for Catastrophic Loss

RMS

Landscape

CLOUD OUTAGE:

LOSS

THE POTENTIAL FOR CATASTROPHIC

2017

Cyber Risk

Landscape Monitoring



2019 Solving Cyber Risk Publication

WILEY



2018 Probabilistic Cyber Assessment



Annual Updates of Our Cyber Risk Outlooks

Occurrence of Data Exfiltration Events by Size







The Changing Face of Cyber Loss

Equifax fined £500,000 over customer data breach

If the security incident had taken place after GDPR came into play, the fine may have been far higher.

GDPR: British Airways faces record £183m fine for customer data breach

Information Commissioner's Office intends to fine airline for "poor security arrangements" - British Airways says it's "surprised and disappointed" by planned penalty.

Facebook to be fined \$5bn for Cambridge Analytica privacy violations - reports

France fines Google \$57 million for European privacy rule breach

The \$5bn fine would be the largest ever levied by the Federal Trade Commission against a technology company

BUSINESS

Marriott Faces \$124 Million Fine Over Starwood Data Breach

Penalty is second hefty fee proposed this week against a major corporation by U.K. enforcer of EU data-privacy rules



CCRS Role in Growth of Cyber Insurance Market

- Cyber risk research at Cambridge Centre for Risk Studies has played an important role in the growth of the cyber insurance market
- CCRS created a cyber exposure data schema
 - Endorsed by Lloyd's
 - Adopted by RMS
 - Selected by ACORD
- CCRS research provided the structure for RMS Cyber Accumulation Management System (CAMS)
 - The leading commercial cyber risk model
- CCRS scenarios adopted by Lloyd's for regulatory accumulation reporting
- CRS scenarios now being created for SE Asia market to boost cyber insurance market there







Lloyd's Business Blackout Scenario: Cyber Attack on US Power Grid



Cyber Terrorism Feasibility in Scenarios



POOI

Judge Business School



Awards and Recognition for CCRS

Cambridge Centre for Risk Studies was honoured to be nominated for awards and invited to be involved in data standards activities, including:



Reactions

CCRS shortlisted for Risk Modeller of the Year, Reactions 2018



2018 Cyber Risk Awards **Pool Re and CCRS** shortlisted for **Cyber Risk Innovation of the Year** for work on developing the Pool Re Cyber Terrorism Extension 2018



ACORD selected the **Cambridge Cyber Exposure Data Schema** (published 2016) to provide to all 4,000+ ACORD members.



ISO 31050 Emerging Risk Standards

CCRS invited to be a member of the British Standards Institution Working Group on scoping the proposed ISO 31050 standard for identifying and managing **Emerging Risks** in business



The Future of Cyber Risk



Today's Sessions on The Future of Cyber Risk

Cyber Risk Landscape



Tom Harvey **Risk Management Solutions**





War Games, Simulations, and Scenarios Justin Clarke-Salt Aon Cyber Solution



Cybergeddon vs. Cybertopia Dr Jennifer Daffron Cambridge Centre for Risk Studies

Cyber Threat Actors







Game Theory Approaches Dr Gordon Woo **Risk Management Solutions**



Journey from Black Hat to White Hat Mike Jones

Security Researcher

Future Technology and Tools



Chair Vincent Gilcreest Tenable.io



Red on Blue: Infinity War Sille Laks **Clarified Security**



Lessons from Telematics: Future Technology & Tools Jasson Casey SecurityScorecard



The Only Limit is Your Imagination Timothy Olsen **Symantec**

Advances in Security



Chair Dr. Raveem Ismail QOMPLX



Managing Cyber Risk in Digital Transformation Stephen Boyer BitSight



Cyber Risk Quantification Prof MingYan Liu University of Michigan



Interdisciplinary Approaches to Cyber Security Dr Jason Nurse University of Kent

Changes in Risk Management



Chair Dave Ruedger **Risk Management Solutions**



The Changing Face of Privacy Law James Clark **DLA Piper**

Changing Workplace Behaviour Stephen Burke Cyber Risk Aware



The Future of Cyber Risk Management in Organisations Domenico del Re PwC UK

Cyber Insurance



Kelly Malynn, **Beazley Group**



Cyber Insurance in 2025 Sarah Stephens FINPRO Cyber, Media & Technology Practice Leader



The Cyber Market's Present and Future Challenges Eric Durand Swiss Re



Future Analytics of Cyber Risk Quantification Dr Christos Mitas Risk Management Solutions



Potential Game-Changers in Future Technologies and Tools

- AI Applied to Malware Development
 - Zero-day vulnerabilities are currently discovered by trial-and-error
 - Hackers are already adopting automation to find vulnerabilities in industry-standard software
 - New classes of malware could evade conventional anti-virus and standard security systems
 - New generations of malware could have rapid evolution or be selforganizing
- Commoditized malware toolkits
 - Reduces skill and cost needed for development
 - Malware-as-a-Service; Ransomware-as-a-service
- Sudden leaps in decryption capability
 - Most of our current security depends on encryption
 - Decryption improvements could jeopardize security standards
 - Quantum computing may enable routine decryption



| | | | To> toxicola | K 17qwv3 | 37qj.₀ | nion |
|---|--|--|--|--|--|--------|
| FOR | SA | LE | | | | |
| Contact tox@sigain | t.org and | l make an | offer: | | | |
| | | | | | | |
| Platform + vir | us; | | | | | |
| DISC DESCRIPTION | and the second second | | construction and an experimental second s | | | |
| Placform + vir | us + dac | abase + to | xicola/awv3/ai.onion priv | /ate kev. | | |
| Platform + vir | us + dac | abase + to | ixicola/qwv3/qj.onion priv | /ate key. | | |
| Platform + vir | us + dac | abase + to | xicola/qwv3/qj.onion priv | /ate key. | | |
| Platform + vir | us + dac | abase + to | xicola/qwv3/qj.onion priv | /ate key. | | |
| Platform + VI Process Explorer - Sysintemaks: | US + OAC | abase + Co nals.com [DES | IXICOLA/QWV3/QJ.ORIOR PRV | vate key. | _ | o x |
| Proterorm + VI Process Explorer - Sysintemals: File Options View Process Fi | US + OAC www.sysinter ind Users | aDase + C nals.com (DES Help | XICOLa / QVIV-3 / QJ.ONION PRI TOP-J68NITG\InfeWorld] | vate key. | - | o x |
| Protectorm + VIF Process Explorer - Sysintematic Options View Process F Details = 0 Detai | WS + Galo www.sysinter ind Users | aDase + Co nals.com (DESi Help | | vate key. | - | 0 X |
| Proterorm + VI Process Explorer - Sysintematic Process File Options View Process File Detrins View Process | WS + data www.sysinter ind Users X 44 6 vate Bytes | aDase + Co nals.com (DESi Help | TOP-J68NITG\InfoWorld] | vate key. | | o X |
| Process Explorer - Sysinternals: Process Explorer - Sysinternals: Process File Options View Process File Decess Decess | US + Calc www.sysinter ind Users X da C vate Bytes | aDase + Co nals.com [DESi Help Working Set | TOP-J68NITG\InfoWorld] PID Description Comp | vate key, | | otal ^ |
| Proterorm + VI Process Explorer - Sysintematic: Options View Process F Decess Trocess Trocess Trocess | WWW.sysinter ind Users X 44 C vate Dytes 2,852 K 3,950 K | Help Working Set | TOP-J68NITG\InfoWorld] PID Description T276 Holt Process for Windows 5 Micro T276 Holt Process for Windows 5 Micro | vate key, | 4 Wrus Tr 0/56 | otal ^ |
| Proterorm + VI Process Explorer - Sysintematic Options View Process File Options View Process wichost axe VSSVC.exe VSSVC.exe VSSVC.exe | US + CAU www.sysinter ind Users X 44 6 vate Bytes 2.852 K 3.960 K 1.884 K | abase + Co nals.com [DESi Help Working Set 5,164 K 9,568 K 3,568 K | TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] PID Description Comp 1276 Host Process for Windows S., Micros 1552 Microsoft® Volume Shedow – Micros 1578 Microsoft® Volume Shedow – Micros | vate key, | 4 VrusTr 0/56 0/56 | otal ^ |
| Picktrorm + Vir Process Explorer - Sysinternals Process Dia Dia D | US + GAU www.sysinter ind Users X 44 6 vate Bytes 2,852 K 3,960 K 1,884 K 8,180 K | ADASE + Co nals.com [DESI Help Working Set 5,164 K 9,568 K 3,648 K 3,648 K | TOP-J68NITG\InfoWorld] PID Description Comp 1276 Host Process for Windows S Micros 1716 Host Process for Windows S Micros 1716 Host Process for Windows S Micros 1718 Host Process for Windows S Micros | valte key. | 4 Vnus Tr 0/56 0/56 0/56 | o X |
| Process Explorer - Sysintemats: u | US + OAU www.sysinter ind Users X 44 6 vate Bytes 2,852 K 3,960 K 1,884 K 8,180 K 9,096 K | abase + C nals.com (DES) Help Working Set 5.164 K 9.568 K 3.648 K 5.016 K 21.084 K | TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] PID Description Comp 1276 Host Process for Windows 5 | vate key, any Name oft Corporation oft Corporation oft Corporation oft Corporation | 4 Wrus Tr 0/55 0/55 0/55 0/55 | otal A |
| Process Explorer - Sysinternals: Process Explorer - Sysinternals: File Options View Process File Process In wichost awa In VSSVC ase In wichost awa In Whoth awa | US + CAU www.sysinter ind Users X 44 6 vate Bytes 2,852 K 3,950 K 1,884 K 8,180 K 9,096 K 118,780 K | ADASE + Co nals.com (DES) Help Working Set 5,164 K 9,569 K 3,648 K 5,016 K 21,084 K 21,084 K 21,084 K | TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] PID Description Comp 1276 Host Process for Windows S Micros 1552 Microsoft® Volume Shedow – Micros 1812 Spooler Sub-System App 2036 Host Process for Windows S Micros 1812 Spooler Sub-System App 2036 Host Process for Windows S Micros 1812 Actualities Service Execut. Micros 1812 Actualities Service Execut. Micros | vate key. | 4 VrusTi 0/55 0/55 0/55 0/55 | ctal ^ |
| Process Explorer - Sysintemate: Process File Options View Process File @ | US + CAU www.sysinter ind Users X 44 5 2.852 K 3.960 K 1.884 K 8.180 K 9.096 K 118.780 K 1.572 K | abase + C nals.com [DESI Help Working Set 5,164 K 9,568 K 3,648 K 5,016 k 21,084 K 60,724 K 3,500 k | TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] Description T276 Host Process for Windows 5 Micror 1716 Host Process for Windows 5 Micror 1716 Host Process for Windows 5 Micror 1512 Artimatives Enrice Execut Micror 1512 Artimativ | valle key. | 4 Virus Tr 0/56 0/56 0/56 0/56 0/56 | otal ^ |
| Process Explorer - Sysintemats: v Process worknot.axe | US + CAU www.sysinter ind Users X 44 6 vate Bytes 2.852 K 3.960 K 1.884 K 8.180 K 1.884 K 9.096 K 118,780 K 1.672 K 7.252 K | ADASE + Co nals.com [DESI Help Working Set 5,164 K 9,568 K 3,648 K 5,016 K 21,084 K 60,724 K 3,500 K 15,036 K | TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] PID Description Comp 1276 Hott Process for Windows S., Micros 1552 Microsoft* Volume Shedow Micros 1552 Spooler SubSystem App 1812 Spooler SubSystem App 1812 Spooler SubSystem App 1812 Antimalivare Service Execut., Micros 1812 Antimalivare Service Execut., Micros 1814 Appatheness for Windows S., Micros 1815 Antimalivare Service Execut., Micros 1814 Appatheness for Windows S., Micros 1815 Antimalivare Service Execut., Micros 1814 Appatheness for Windows S., Micros 1815 Antimalivare Service Execut., Micros 1814 Appatheness for Windows S., Micros 1815 Antimalivare Service Execut., Micros 1814 Appatheness for Windows S., Micros 1815 Antimalivare Service Execut., Micros 1814 Appatheness for Windows S., Micros 1815 Antimalivare Service Execut., Micros 1814 Appatheness for Windows S., Micros 1815 Antimalivare Service Execut., Micros 1814 Appatheness 1815 Appathenes 1815 Appathene 1 | vate key, any Name oft Corporation and Corporation and Corporation and Corporation and Corporation and Corporation and Corporation | 4 Vrus Tr 0/55 0/55 0/55 0/55 0/55 0/55 | otal ^ |
| | US + CdC www.sysinter ind Users X J Sec 2,852 K 3,950 K 9,056 K 118,700 K 1,872 K 7,252 K 7,252 K 2,905 K | aDaSe + C nals.com [DES] Help → Working Set 5,164 K 9,568 K 3,648 K 5,016 K 21,084 K 60,724 K 60,724 K 3,500 K 15,036 K 15,036 K 22,788 K | TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] PID Description Comp 1276 Host Process for Windows S Micros 1552 Microsoft® Volume Shedow - Micros 1812 Spooler Sub-System App 1276 Host Process for Windows S Micros 1812 Applicationse Service Execut Micros 1812 Antimisme Service Execut Micros 1812 Antimisme Service Execut Micros 1824 Host Process for Windows S Micros 1832 Host Process for Windows S Micros 1830 Microsoft Windows Service Execut. In Micros 1830 Microsoft Windows Service Host Process 1840 Microsoft Micros 1840 Microsoft 1840 Mi | vary Name off Corporation off Corporation off Corporation off Corporation off Corporation off Corporation off Corporation | 4 What Tr 0/55 0/55 0/55 0/55 0/55 0/55 0/55 | otal |
| | US + GAD www.sysinter ind Users × 44 0 2.852 K 3.950 K 1.884 K 9.096 K 118,780 K 1.572 K 2.952 K 1.572 K 2.952 K 1.512 K | ADASE + Comparison of the second seco | TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] PID Description T275 Host Process for Windows 5 Micror T716 Host Process for Windows 5 Micror T716 Host Process for Windows 5 Micror T716 Anst Process for Windows 5 Micror T1512 Antimaliwae Service Execut Micror 3332 Host Process for Windows 5 Micror 3332 Micror Time Search P Micror 33312 Micror Time Search P Micror | vate key, sany Name off Corporation soft Corporation soft Corporation soft Corporation soft Corporation soft Corporation soft Corporation soft Corporation soft Corporation | * VrusTr 0/55 0/55 0/55 0/55 0/55 0/55 0/55 0/5 | otal X |
| Process Explorer - Sysintemate v Process Explorer - Sysintemate v Tile Options View Process F With I and I I I I I I I I I I I I I I I I I I I | US + Gal www.sysinter ind Users x db c 2.852 K 3.660 K 1.884 K 8.180 K 9.956 K 118.780 K 1.672 K 29.052 K 1.912 K 1.215 K | ADASE + Co nals.com [DESI Help Working Set 5.164 × 9.568 × 3.648 × 5.016 × 21.084 × 21.084 × 3.500 × 16.036 × 22.788 × 10.228 × 5.500 × | TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] PID Description Comp T276 Hott Process for Windows S Micror T652 Microsoft* Volume Shedwar S Micror T161 Societ Process for Windows S Micror T181 Spooler SubSystem App T181 Actimatives Service Execut. Micror T181 Actimatives Service Execut. Micror T3204 Hott Process for Windows S Micror T3304 Microsoft Windows Search F Micror T3310 Microsoft Windows Search F Micror T3812 Microsoft Windows Search F Micror T3812 Microsoft Windows Search F. Micror T3812 Microso | vate key, any Name off Corporation off Corporation | | o X |
| Process Explorer - Sysinternals: Process Process wichoat axe vSSVC ase wichoat axe wichoat | US + 030 www.sysinter ind Users X 04 0 2.852 K 3.860 K 1.870 K 1.870 K 1.672 K 7.252 K 2.9052 K 1.912 K 1.912 K 1.912 K 1.912 K | aDaSe + C mals.com (DESI Help → Working Set 5,164 × 9,568 × 3,648 × 5,016 × 21,084 × 10,228 × 5,800 × 10,228 × 21,228 × 21,228 × | TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] TS2 Hoat Process for Windows 5 Micros TS2 Actionative Service Security Micros TS12 Actinatives Service Security Micros 3324 Hoat Process for Windows 5 Micros 3324 Microsoft Windows Search F Micros 3328 Microsoft Windows Search F Micros 3328 Microsoft Windows Search F Micros 3428 Microsoft Windows Search F Micros 3428 Microsoft Windows Search F Micros 3438 Microsoft Windows Search F Micros 344 Microsoft Windows Search F Micros 345 Microsoft Windows Search F Micros 346 Microsoft Windows Search F Micros 347 Microsoft Windows Search F Micros 348 Microsoft Windows Search F Micros 349 Microsoft Windows Search F Micros 340 Microsoft Windows Search F Micros 340 Microsoft Windows Search F Micros 341 Microsoft Windows Search F Micros 342 Microsoft Windows Search F Micros 343 Microsoft Windows Search F Micros 344 Microsoft Windows Search F Micros 345 Microsoft Windows Search F Microsoft Windows 345 Microsoft 345 | vary Name off Corporation off Corporation off Corporation off Corporation off Corporation off Corporation off Corporation off Corporation off Corporation | 4 Waa Ti 0/255 0/255 0/255 0/255 0/255 0/255 0/255 0/255 0/255 | otal * |
| Process Explorer - Sysinternals: Process File Options View Process File Options View Process wchost.exe sychost.exe | US + GAU www.sysinter ind Users X 446 C 2.852 K 3.550 K 1.884 K 8.180 K 9.055 K 1.872 K 2.9.052 K 1.872 K 1.972 K 1.972 K 1.912 K 1.912 K 1.3124 K | ADDASE + Common and the second | XICOL3 / QVV 3 / QLONION DN XICOL3 / QVV 3 / QLONION DN TOP-J68NITG(InfoWorld] PID Description T276 Host Process for Windows S Micros T1716 Host Process for Windows S Micros T1716 Host Process for Windows S Micros T1712 Administre Service Execut Micros 3204 Host Process for Windows S Micros 3320 Host Process for Windows S Micros 3320 Host Process for Windows S Micros 3320 Host Process for Windows S Micros 3321 Microsoft Windows Search P Micros 3321 Microsoft Windows Search P. Micros 368 Microsoft Windows Search P. Micros 368 Microsoft Windows Search P. Micros 364 Microsoft Network Peemich P. Micros 364 Microsoft Network Peemich P Micros 3644 Microsoft Network Results P Micros | valte key, any Name off Corporation off Corporation | 4 Vita Ti 0/55 0/55 0/55 0/55 0/55 0/55 0/55 0/5 | otal * |
| Process Explorer - Sysintemate: v File Options View Process F Options View Process F options View Process wichost.exe | US + Gal www.sysinter ind Users X db C 2.852 K 3.660 K 1.884 K 9.056 K 118.760 K 1.572 K 29.052 K 1.912 K 1.216 K 9.192 K 1.312 K 1.312 K | Addase + Co mals.com [DESI Help Working Set 5.164 × 9.568 × 3.648 × 5.164 × 9.568 × 3.648 × 5.1084 × 60.724 × 3.500 × 16.036 × 16.036 × 22.788 × 10.228 × 5.800 × 5.8000 × 5.800 × 5.800 × 5.8000 × 5.8000 × 5.8000 × | TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] PID Description PID Description PID Description Pionum Comparison Pionum | vate key, any Name off Corporation off Corporation | | otal 1 |
| Process Explorer - Sysintematics Process Process worknott.exe worknott.exe worknott.exe worknott.exe worknott.exe worknott.exe worknott.exe Search/RetricolHost.exe worknott.exe work | US + GAU www.sysinter ind Users X 44 6 2.852 K 3.860 K 1.884 K 8.180 K 1.870 K 1.772 K 2.9052 K 1.912 K 1.912 K 1.1716 K 1.121 K 1.1 | ADASE + C mals.com [DES] Help Working Set 5.164 K 5.016 K 21.084 K 60.724 K 3.500 K 22.788 K 10.228 K 5.000 K 22.788 K 5.000 K 22.788 K 5.000 | XICOL3 / QVV 3 / QLONION DM XICOL3 / QVV 3 / QLONION DM TOP-J68NITG\InfoWorld] PID Description Comp Z75 Host Process for Windows 5 Micror T276 Host Process for Windows 5 Micror T161 Antimume Service Execut Micror 3206 Host Process for Windows 5 Micror 3320 Host Process for Windows 5 Micror 3320 Microsoft Windows Search F Micror 3320 Microsoft Windows Search F Micror 3320 Microsoft Windows Search F Micror 3412 Microsoft Windows Search F Micror S414 Microsoft Networks Featme L. Micror S44 Local Security Kuthony Foc Micror | vary Name off Corporation off Corporation | 4 What Ti 0/25 0/25 0/25 0/25 0/25 0/25 0/25 0/25 | otal * |
| Process Explorer - Sysintemate: Process Process Process Process Process Process Process without awa | US + GAU www.sysinter ind Users X 446 C 2.852 K 3.550 K 1.884 K 8.180 K 9.055 K 1.870 K 1.870 K 1.672 K 1.972 K 1.972 K 1.912 K 1.912 K 1.912 K 1.312 K 1.31 | Addase + Communication of the second | TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] PID Description T276 Holt Process for Windows 5 Micror T176 Host Process for Windows 5 Micror T161 Spooler SubSystem App T161 Appoint Process for Windows 5 Micror T161 Anot Process for Windows 5 Micror T164 Microsoft Windows Search F Micro T164 Microsoft Windows Search F Micro T164 Host Process for Windows 5 Micror T164 Host Process for Windows 5 Micro T164 Host Proce | valte key, any Name off Corporation off Corporation | * Waa Ti 0/55 0/55 0/55 0/55 0/55 0/55 0/55 0/5 | otal * |
| Process Explorer - Sysintemate v Process Process P Process wichost ave wichost ave | US + Gal www.sysinter ind Users X 04 6 2.852 K 3.960 K 1.884 K 1.872 K 9.956 K 118,780 K 1.725 K 9.952 K 1.912 K 1.215 K 9.192 K 1.312 K 1.325 K 1.355 K 1.3 | Addase + Comparison (DES) Help Working Set 5,164 × 9,568 × 3,648 × 5,164 × 9,568 × 3,648 × 5,016 × 21,084 × 21,084 × 16,036 × 22,788 × 10,028 × 5,800 × 22,788 × 10,228 × 5,800 × 5,916 × 5,917 × 5,91 | TOP-J68NITG\InfoWorld] TOP-J68NITG\InfoWorld] PID Description Comp T276 Hott Process for Windows S Micros T652 Microsoft® Volume Studies T1652 Microsoft® Volume Studies T1612 Actimalisme Service Execut. Micros T1812 Actimalisme Service Execut. Micros T1814 Host Process for Windows S Micros T1814 Microsoft Windows Search P. Micros T1844 Microsoft Windows Search F. Micros T1844 Microsoft Network Reature L. Micros T844 Microsoft Network Reature L. Micros T644 Microsoft Network Reature Microsoft Network T644 Microsoft T644 | vary Name off Corporation off Corporation | 4 WearT 0/55 0/55 0/55 0/55 0/55 0/55 0/55 0/5 | otal * |
| Process Explorer - Sysintemates Process workost ave workost | US + GAU www.sysinter ind Users X 44 6 2.852 K 3.960 K 1.884 K 8.180 K 1.894 K 9.096 K 118.70 K 1.727 K 9.095 K 1.727 K 1.912 K 1.716 K 9.192 K 1.312 K 1.312 K 1.312 K 1.312 K 1.312 K 1.328 K 1.432 K 1.452 K 1.45 | Addase + C mals.com [DES] Help Working Set 5.164 K 5.164 K 5.168 K 21.084 K 60.724 K 3.500 K 22.788 K 10.228 K 5.800 K 21.228 K 5.800 K 21.228 K 5.916 K 6.524 K 6.52 | XICOL3 / QVV 3 / QLONION DM XiCOL3 / QVV 3 / QLONION DM TOP-J68NITG\InfoWorld] PID Description T276 Host Process for Windows 5 Micror T276 Host Process for Windows 5 Micror T161 Antimumer Service Execut Micror 3026 Host Process for Windows 5 Micror 3020 Host Process for Windows 5 Micror 504 Host Process for Windows 5 Micror 504 Host Process for Windows 5 Micror 504 Host Process for Windows 5 Micror 3040 Descript Microl ProcMicror 3040 Descript Microl ProcMicror 3040 Descript Microl Manager Micro | vate key, any Name off Corporation off Corporation | 4 What Ti 0/55 0/55 0/55 0/55 0/55 0/55 0/55 0/5 | otal * |

37,936 K

2,780 K

46.658 K

11,216 K

16.612 K

6.604 K

2.892 K

14,764 K

MSASCulL exe

wordpad exe

CoeDrive eve

MpCmdRun exe

DriverUpdate ext

ргосеф64 ехе

PCHealthBoost.exe

111.888 K

27.820 K

36 216 K

37.600 K

41 644 K

9,644 K 5656 Windows Defender notificati... Microsoft Corporation

4852 Sysintemals Process Explo

7032 Microsoft Malware Protection

4124 Micmanft OneDrive

3952 Windows Wordpad Application Microsoft Compration

0/56 4/57 0/57 0/56

0/55

0/55

Changes in the Business Models of Threat Actors

- The equilibrium between cyber attackers and defenders is finely balanced
 - Defenders are increasing their security expenditure and learning to combat hacker techniques
 - Attacker evolve new techniques to exploit other weaknesses
- Hackers could decisively gain the upper hand through:
 - Reduction in cost/skill needed for attacks (commoditized malware)
 - Improved rewards for a successful hack (bigger ransoms get paid)
- Many more well-educated hackers become active, as an alternative to increasing graduate youth unemployment
- Dark web IPv6 provides much larger hacker safe havens for hackers to operate from
- Surge of independent attacks by many more actors adopting hacking as a profession.
 - Probably inexperienced initially (lower severities) but rapidly increasing in success and impact







The Gloves Come Off Nation-State Cyber Teams

- Fear of retaliation and political restraint currently prevent foreign nation-state cyber teams from attacks on West that are too overt or damaging
 - We are currently in a cyber 'Cold War'
 - Russia, China, North Korea operate cyber attacks against US & European private sector companies
 - They are capable of more severe and intensive campaigns if the gloves came off
- Geopolitical events could turn the cold war hot
 - e.g. Military attack against North Korea/Iran
 - Growingly hostile political postures
- Nation states could target private sector and disguise their tracks to make attribution difficult
- Resources, capabilities and tools available to nation state hackers would result in much more severe and extensive attacks







Advances in Security and Corporate Risk Management

- New security technologies offer hope of AI-led protection
 - Potential for improved effectiveness and affordability
- Cyber security investment is prioritized
 - Targeted on measures that are proven to be most effective
 - Costs of effective security reduces and is widely implemented
- Full recognition of the human dimension of cyber risk
- Moves by companies to share information, improve human capital, redefine trust networks, use AI
- Switch to cloud for digital economy
 - May result in highly secure, low-loss environment
 - Security-as-a-Service more secure than on-premises
- What will it take for most organisations to achieve '6-Sigma' protection levels?
 - Minimal tolerance of loss from cyber
 - Managed breach tolerance



Risk Studies





Radical Upgrade of Global Cyber Law Enforcement

- Conviction of criminals will reduce cyber crime but requires substantial efforts to do this
 - International agreements to prosecute in foreign jurisdictions
 - Training police forces in cyber crime detection
- The past year has seen one of the lowest conviction rates for cyber criminals in recent years despite record levels of cyber crime
 - Law enforcement has real challenges in bringing criminal hackers to justice
 - Conviction rates are the main deterrent for crime
- There are key initiatives to improve cyber law enforcement around the world that could result in a major reduction in cyber crime
- Frequency of cyber crimes would reduce, and the ambient level of cyber risk would reduce







Conclusions: The Future of Cyber Risk

- Many factors will determine the future of cyber risk the level of future loss
- This conference brings together many different disciplines and areas of expertise to explore the factors that will determine the future of cyber risk
- Our intention is to use these contributions to set out the issues and help organizations plan for the coming years ahead
- The Cambridge Centre for Risk Studies has contributed to the thought leadership in the understanding of cyber risk over the past decade
- The Cambridge Centre for Risk Studies intends to contribute to the understanding of cyber risk as it changes over the next decade



Centre for **Risk Studies**

