Cybersecurity van infrastructuur

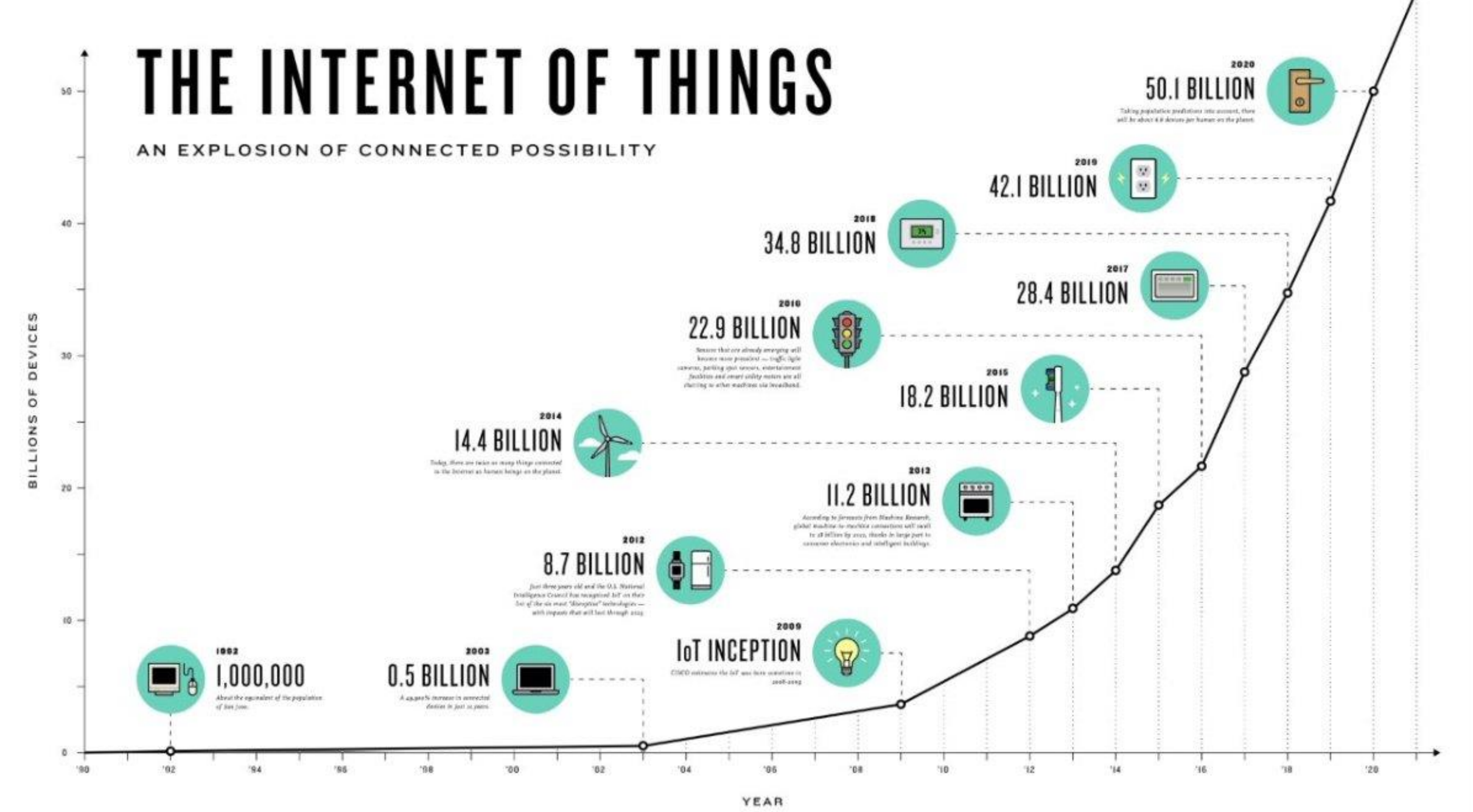
Masterclass IenW
22 februari 2018

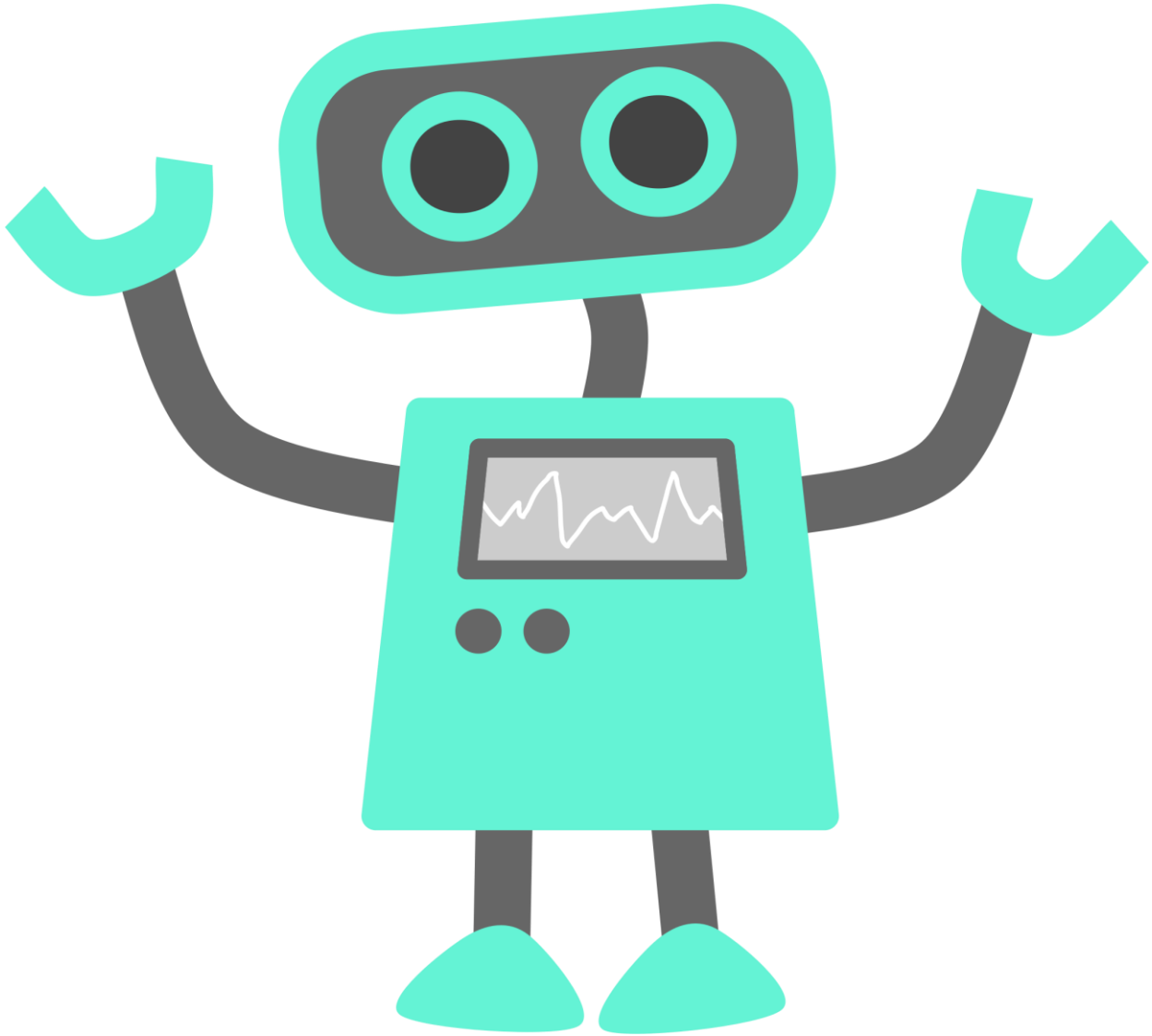
Michel van Eeten

TU Delft

THE INTERNET OF THINGS

AN EXPLOSION OF CONNECTED POSSIBILITY





Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

Cyber Security Strategie

Herijking 2017

Bewustwording

De Security awareness wordt in 2018 structureel gestimuleerd in samenwerking met communicatie en HR met gebruik van

De mens vormt de zwakste schakel in de beveiligingsketen. Technische maatregelen tegen dreigingen kunnen genomen zijn, maar als een medewerker, leverancier of ketenpartner op een website komt met malware, kan een besmetting razendsnel om zich heen grijpen.

Bewustwording

De medewerker of ketenpartner moet zich bewust zijn van zijn eigen rol en verantwoordelijkheid in de beveiliging van informatie en systemen.

De bewustwording wordt op verschillende manieren vormgegeven. Het geven van trainingen blijkt effectief. Ook het herhaaldelijk oefenen van de handelingswijze bij cyberincidenten draagt bij aan een hoge mate van bewustzijn.
Onderhoudsaannemers nemen ook deel aan trainingen en oefeningen, want zij hebben een belangrijke rol in de afhandeling van incidenten. Een belangrijk deel van bewustwording is het kennen van de eigen business en de cyber risico's daarvoor.

Trainen en Leren

Resultaten van oefeningen worden gedeeld met de organisatie. Vervolgens worden

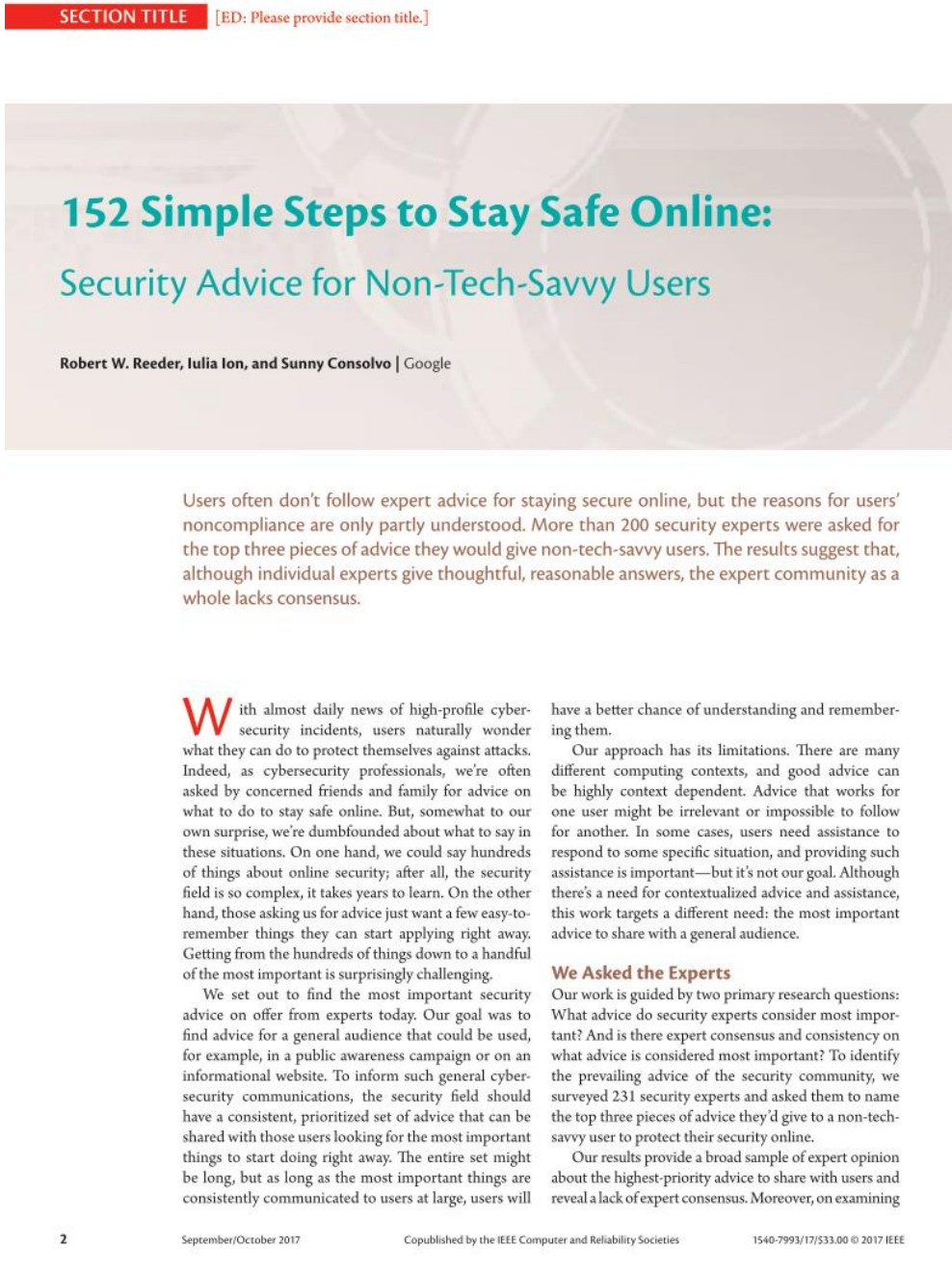
PEBKAC

Problem Exists Between Keyboard and Chair

TU Delft

Mens is niet het probleem

- Onderzoekers vroegen 231 security experts naar hun top 3 adviezen voor niet-technische gebruikers. Ze kregen 837 (!) adviezen...
- US CERT publiceerde rapport met adviezen voor niet-technische gebruikers: 57 pagina's met 534 adviezen.
- Negeren van adviezen is dus onvermijdelijk
- Gebruikers zijn niet de zwakste schakel, maar de laatste schakel



SECTION TITLE [ED: Please provide section title.]

152 Simple Steps to Stay Safe Online:

Security Advice for Non-Tech-Savvy Users

Robert W. Reeder, Iulia Ion, and Sunny Consolvo | Google

Users often don't follow expert advice for staying secure online, but the reasons for users' noncompliance are only partly understood. More than 200 security experts were asked for the top three pieces of advice they would give non-tech-savvy users. The results suggest that, although individual experts give thoughtful, reasonable answers, the expert community as a whole lacks consensus.

With almost daily news of high-profile cybersecurity incidents, users naturally wonder what they can do to protect themselves against attacks. Indeed, as cybersecurity professionals, we're often asked by concerned friends and family for advice on what to do to stay safe online. But, somewhat to our own surprise, we're dumbfounded about what to say in these situations. On one hand, we could say hundreds of things about online security; after all, the security field is so complex, it takes years to learn. On the other hand, those asking us for advice just want a few easy-to-remember things they can start applying right away. Getting from the hundreds of things down to a handful of the most important is surprisingly challenging.

We set out to find the most important security advice on offer from experts today. Our goal was to find advice for a general audience that could be used, for example, in a public awareness campaign or on an informational website. To inform such general cybersecurity communications, the security field should have a consistent, prioritized set of advice that can be shared with those users looking for the most important things to start doing right away. The entire set might be long, but as long as the most important things are consistently communicated to users at large, users will have a better chance of understanding and remembering them.

Our approach has its limitations. There are many different computing contexts, and good advice can be highly context dependent. Advice that works for one user might be irrelevant or impossible to follow for another. In some cases, users need assistance to respond to some specific situation, and providing such assistance is important—but it's not our goal. Although there's a need for contextualized advice and assistance, this work targets a different need: the most important advice to share with a general audience.

We Asked the Experts

Our work is guided by two primary research questions: What advice do security experts consider most important? And is there expert consensus and consistency on what advice is considered most important? To identify the prevailing advice of the security community, we surveyed 231 security experts and asked them to name the top three pieces of advice they'd give to a non-tech-savvy user to protect their security online.

Our results provide a broad sample of expert opinion about the highest-priority advice to share with users and reveal a lack of expert consensus. Moreover, on examining

 Copublished by the IEEE Computer and Reliability Societies 1540-7993/17/$33.00 © 2017 IEEE


‘Human error’ is in veiligheidskunde al decennia geleden afgeserveerd...

BIR (BIR:2012 -> BIR2017)

Zowel nieuwe als bestaande diensten, producten en werken moeten voldoen aan de BIR.

Eind 2017 is de nieuwe versie van de BIR

BIR is de baseline voor security maatregelen

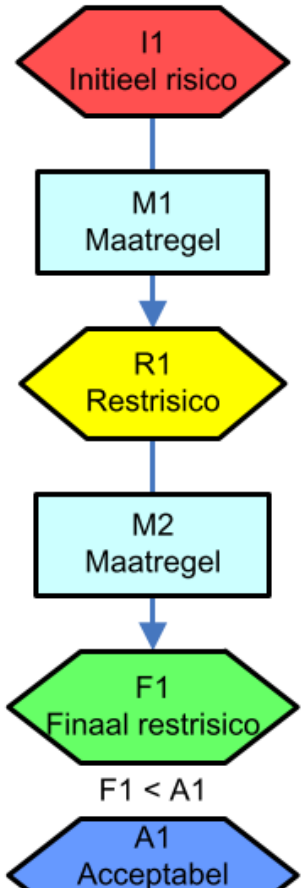
Rijksbreed is bepaald dat de informatiebeveiliging van de IV systemen van de Rijksoverheid minimaal moet voldoen aan het basisniveau dat in regelgeving is opgelegd. Rijkswaterstaat moet voldoen aan de Baseline Informatiebeveiliging Rijksdienst (BIR).

Volgens de BIR is de lijn altijd zelf verantwoordelijk voor de beveiliging van zijn mensen, processen en middelen. Het security centre adviseert hoe zij de digitale beveiliging moeten inrichten. De Baseline volstaat in de regel voor de IV.

Voor Missie Kritieke Systemen en Industriële Automatisering bepaalt het security centre met de eigenaar van het systeem tijdens een "quick scan risicoanalyse" of extra beveiliging noodzakelijk is. Hier zijn ook aanvullende cyber security implementatie richtlijnen Rijkswaterstaat (CSIR) ontwikkeld en geïmplementeerd.

Proceseigenaren mogen van de basismaatregelen afwijken, mits zij het restrisico voor hun proces inzichtelijk hebben gemaakt, vastleggen en accepteren. Ook de

Restrisico's



Restrisico's inzichtelijk maken

Risicomanagement betekent voor Rijkswaterstaat inzicht hebben in de belangrijkste IV systemen (impact) en sturen op het verminderen van de (rest)risico's voor deze systemen tot een acceptabel restrisico. Dit is een risico gestuurde aanpak. In het algemeen volstaat de baseline om de risico's voor de geëiste beschikbaarheid, integriteit en vertrouwelijkheid voldoende af te dekken.

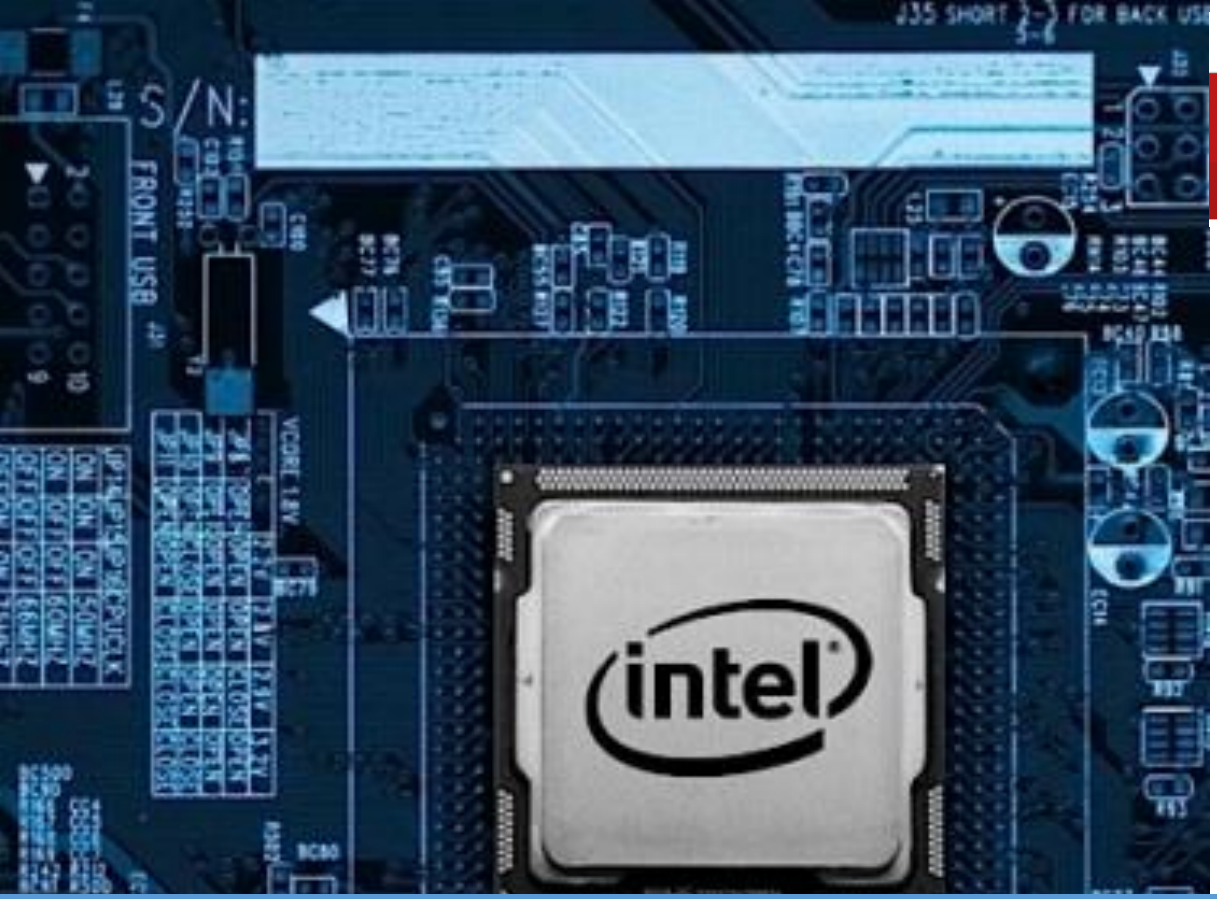
Voor Missie Kritieke Systemen en Industriële Automatisering bepaalt de eigenaar van het systeem met het security centre of extra beveiliging noodzakelijk is, om risico's nog verder te beperken tot een acceptabel niveau.

De meeste ICT-ontwerpen gaan wel in op de verschillende beveiligings-maatregelen die getroffen zijn, maar geven geen inzicht in hun samenhang en de restrisico's die overblijven. Om de restrisico's inzichtelijk te krijgen maakt Rijkswaterstaat gebruik van Risico Reductie Overzichten. Een Risico Reductie Overzicht maakt een complex probleem inzichtelijker voor reviewers, auditors,

risico = kans x gevolg

weten we niet

weten we ook niet



BBC Sign in News Sport Weather Shop Earth Travel More

NEWS

Home Video World UK Business Tech Science Stories Entertainment & Arts Health

Technology

Hackers 'could target electricity grid' via solar panel tech

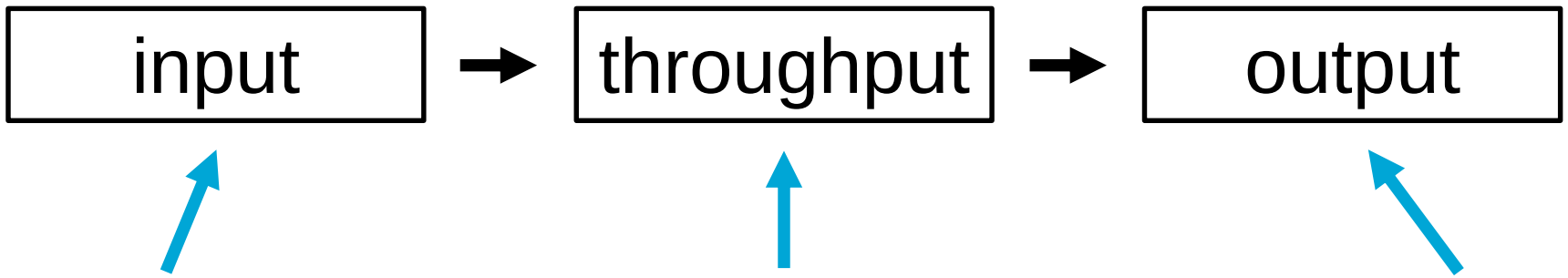
By Chris Baraniuk
Technology reporter

8 August 2017 Share

we kennen onze eigen systemen niet

we zijn afhankelijk van andermans systemen

hoe ‘meten’ we risico?



hoeveel maatregelen we nemen
(bv. maturity model)

hoe druk we daarmee zijn
(bv. hoeveel incidenten afgehandeld)

daadwerkelijke risico
(grotendeels onmeetbaar)

Hoe verder?

- De cybersecurity strategie is goede basis
- Neem afscheid van "mens als zwakste schakel"
- Beveiliging die niet kan omgaan met menselijk falen, is geen beveiliging
- Staar je niet blind op "baseline" en "restrisico's"
- Zoek actief naar wat je niet weet, naar verrassingen ("dat zou niet moeten kunnen")
- Gebruik buitenstaanders (hackers, onderzoekers)
- Verschuif middelen van audit en compliance naar veerkracht en improvisatie

TU Delft


Dank u!
Contact via
m.j.g.vaneeten@tudelft.nl
TU Delft