Cyberrisiko for internrevisorer

WEBINAR OM CYBERSIKKERHET, IIA, 2021-04-15

Chris Culina

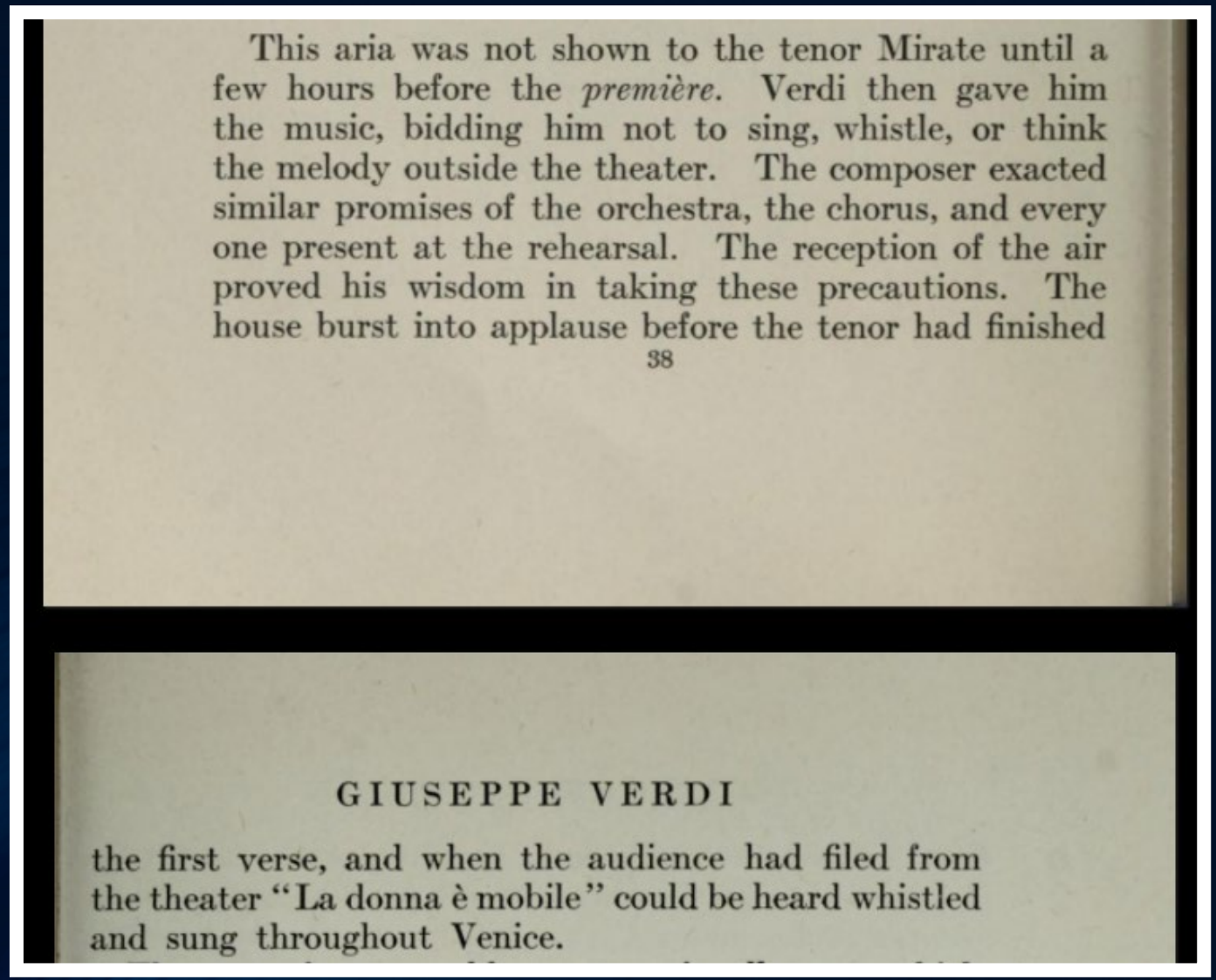
- Daglig leder, sikkerhetsrådgiver, hendelseshåndterer, trusseletterretningsanalytiker og renholdsansvarlig i eget, nystartet selskap
- Tidligere KPMG, BDO, NSM og ymse annet
- Operativ og teknisk bakgrunn
- Bistår primært virksomheter med hendelses- og trusselhåndtering, men også rådgiving innen cybersikkerhet og beredskap
- Still spørsmål i chat, så tar vi det når det passer

secunor

Verdi og verdivurdering

Alle kjenner Verdis "La Donna è mobile", om enn fra reklamer for "autentiske" pizzaer og pastasauser.

Få vet at Verdi hadde et godt grep om informasjonssikkerhet, og forstod verdien av det han hadde skapt, samt at denne verdien måtte beskyttes.



This aria was not shown to the tenor Mirate until a few hours before the *première*. Verdi then gave him the music, bidding him not to sing, whistle, or think the melody outside the theater. The composer exacted similar promises of the orchestra, the chorus, and every one present at the rehearsal. The reception of the air proved his wisdom in taking these precautions. The house burst into applause before the tenor had finished

38

GIUSEPPE VERDI

the first verse, and when the audience had filed from the theater "La donna è mobile" could be heard whistled and sung throughout Venice.

Alle virksomheter har verdier

- Finansielle verdier
- IPR
- Know-how
- Operativ evne
- Omdømme
- Strategisk Verdi
- Personopplysninger
- Og
- Mange
- Mange
- Flere
- Seriøst
- Vi kunne
- Holdt på lenge

Virksomheter har problemer med å identifisere verdiene sine

- Hvordan i all verden skal du kunne beskytte noe du ikke vet at du har?

Med verdi følger risiko

- Det snakkes om ulike typer risiko
  - Finansiell risiko
  - Omdømmerisiko
  - Informasjonsrisiko
  - Cyberrisiko…
- Det kan være nyttig, så lenge man ikke er at den oppfatning at cyberrisiko er noe IT-avdelingen driver med og har ansvar for.

Hvis det kan påvirke, og potensielt velte, virksomheten, er det definitivt virksomhetsrisiko, og det tilligger virksomhetsstyringen.

Cyberrisiko oppsummert

- Datakriminalitet har utviklet seg fra en eksklusiv klubb bestående av eksperter og nasjonalstater til et lovløst lykkeland for opportunister.
- Denne utviklingen har medført en endring i trusselbildet i retning av det kaotiske.
- Bredden blant trusselaktørene gjør at motivasjonen er variert.
- Internetts grenseoverskridende natur gjør at geografisk lokasjon har liten betydning.
- Kort oppsummert; Alle har digitale verdier som er interessante for noen, og en motivert trusselaktør kan med lav kostnad og risiko ramme verdiene fra hvor som helst i verden, når som helst.

Risikoforståelse

- Risikoforståelsen bygger på empiri
  - Vi vet at det finnes en trussel
  - Vi vet at det finnes sårbarheter
  - Vi vet at verdier kan gå tapt
- Brann er et godt eksempel
  - De færreste kommer til å oppleve brann
  - Alle tar likevel brannforebyggende tiltak som en selvfølge
  - Penger ut av vinduet?
- Cyberrisiko er problematisk – mangler empiri og fysiske egenskaper

Omgåelse av problemet

- Tillegg slips-vennlige, fysiske egenskaper for å stille viktige spørsmål
  - Kan Windows knuses?
  - Kan man gå over eller rundt brannmuren?
  - Kan man bevege seg langsomt nok til at UltraSecure ZX10000 ikke ser deg?
  - Vil vi få vite at en rute knuses, at noen klatrer over muren eller sniker seg forbi en deteksjonsmekanisme?
- Skaff kompetanse
- Unngå å sette bukken til å passe havresekken

Risikoko

- Metodikk, schmetodikk
- Shit in, shit out
- Sannynlighet er problematisk når man har å gjøre med motiverte og tilpasningsdyktige trusselaktører
- Sannsynlighet er problematisk når man ikke vet at man er sårbar
- Usikkerhet knyttet til trussel og sårbarhet må ha en effekt på uttrykt sannsynlighet i tradisjonell tilnærming
- Det er viktigere at det gjøres en vurdering som skaper grunnlag for bevisst handling, enn at Verdens Beste Metode™ benyttes.

Internrevisor til unnsetning

- Virksomhetene må hjelpes til å sette fokus på cyberrisiko
- Forankring av sikkerhetsstyring i virksomhetsstyringen, hos dem som eier risikoen
- Ukentlige nyhetsoppslag bør gi internrevisor gode anledninger til å aktualisere nye problemstillinger i virksomheten
- Kan starte med følgende tre spørsmål:
  - Har virksomheten digitale verdier?
  - Har virksomheten et styringsystem for informasjonssikkerhet?
  - Har virksomheten KPI-er på informasjonssikkerhet?

  Er svaret på noe av dette "nei", har man en jobb foran seg.

Spørsmål?

chris@secunor.no

linkedin.com/in/chrisculina/

secunor