

CYBER**NB**

CIP**net**

Critical Infrastructure Protection



What to think about when you leave here today

'cyber is simply another risk category to address'

'risk management principles apply – as with other risks'

'know the right questions to ask – and to whom'

'start with the end in mind'

CYBER**NB**

CIP**net**

Critical Infrastructure Protection

Principles of Risk Management:

Risk Mitigation

- What are the SLA's with in-house or outsourced cybersecurity providers (*MSP / MSSP / MDR / SecOps*)?
- Supply Chain partners all operating with cyber hygiene standards?
 - ISO 27001
 - CAN CSC
 - US CMMC
- Mutual Assistance Agreements?
 - Across municipalities?
 - Across cybersecurity service Providers?



Principles of Risk Management:

Risk Transfer

- Insurance policy? MSP?
 - What does this entail? What should you expect?
 - SLA's?
- Rapid response:
 - Crisis Comms?
 - MSSP / DFIR Services?
 - Negotiation services?
 - "self-insure vs insure?
 - Ransom payment limits?



https://cybernb.ca/userContent/documents/Programs/Trust%20&%20Compliance/CyberNB_CyberInsurance.pdf

Principles of Risk Management:

Risk Acceptance

- Based on risk assessment:
 - Do you accept the exposure of any gaps identified?
 - Does that meet the contract compliance of the insurance policy?
 - Do you know the costs of mitigation and monitoring as compared to the cost of risk acceptance?

Do you know what exposures you are accepting today?





Today, could be a bad day...

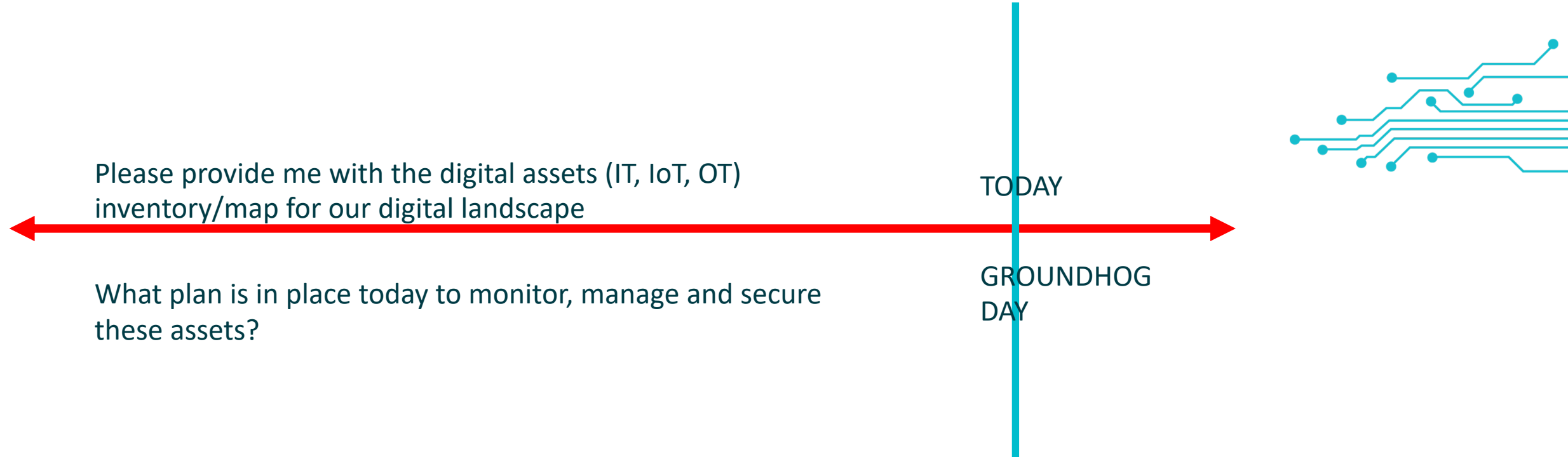
CYBER**NB** | CIPnet



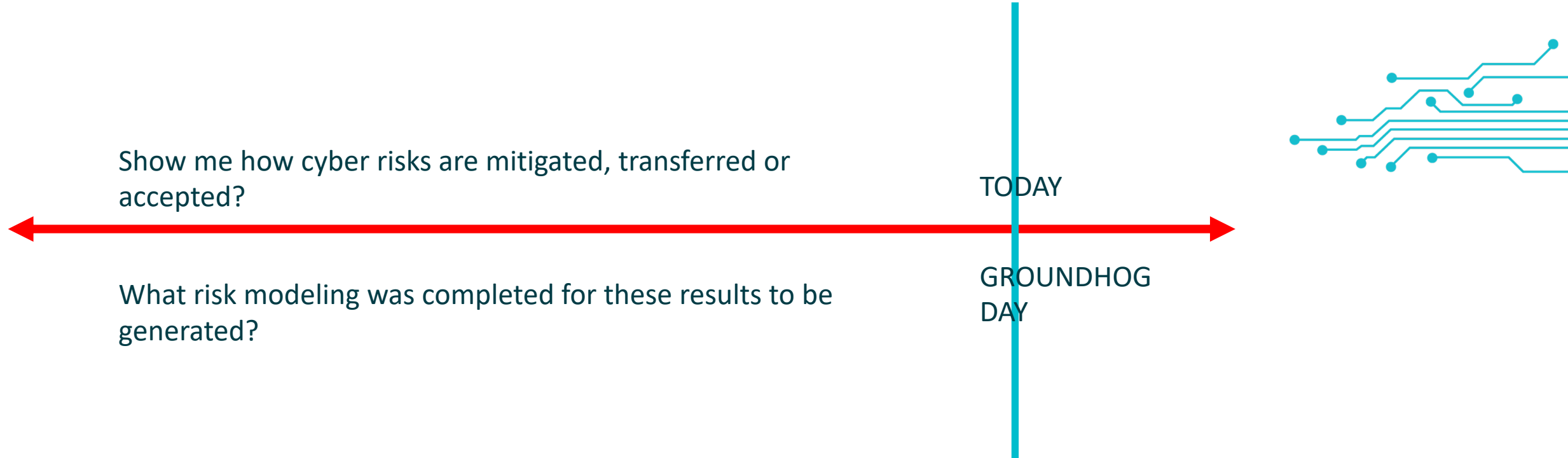
Things to consider and ask...



...to avoid the inevitable event...



...that will otherwise occur...



...ready or not...

How are cyber risks identified and managed for projects we are planning in the future?



What is the additional cost to manage cyber threats for these new initiatives and how has this been factored into the budget?

TODAY

GROUNDHOG
DAY



...So, will you be able to avoid or reduce impact...

Please show me the results from our last pen test on our digital assets.

Please show me the employee awareness training plan for all staff



TODAY

GROUNDHOG
DAY

Please show me the SLA's with our internal / external SOC operations team for identification and notification of incident.

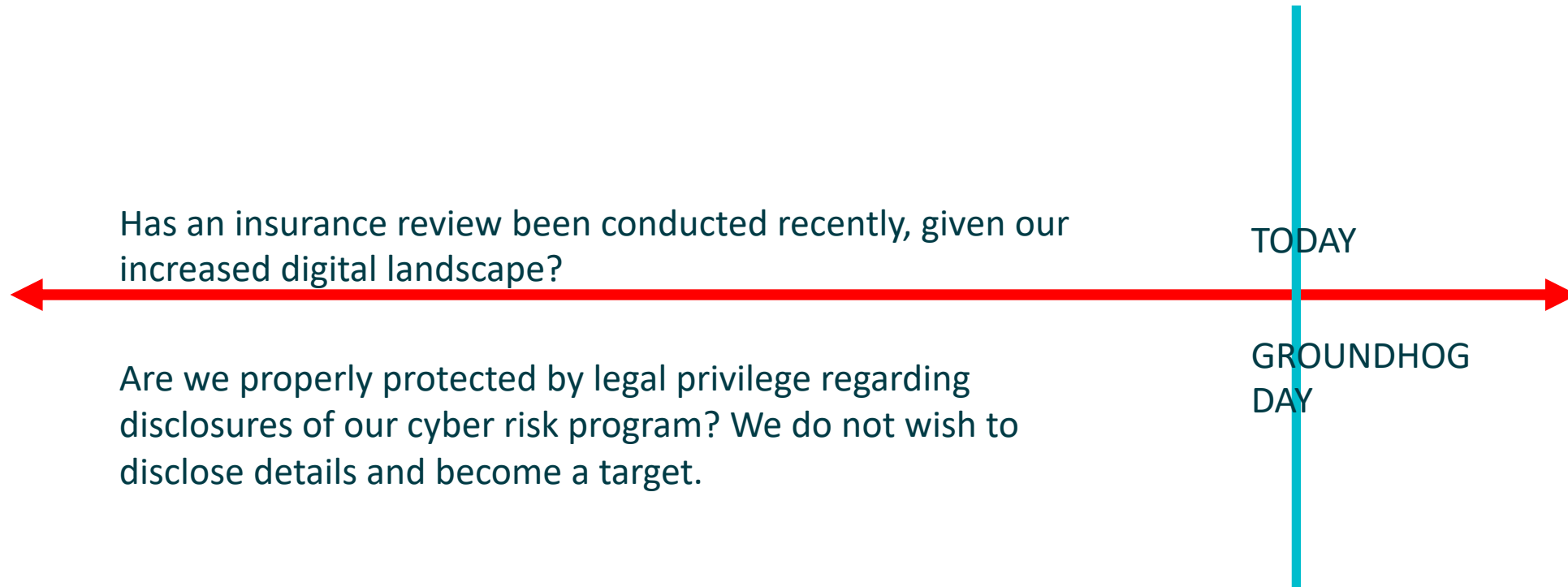
Who is watching out for us 24/7 365?



...when the day arrives...



...rather than be a victim of unpreparedness...



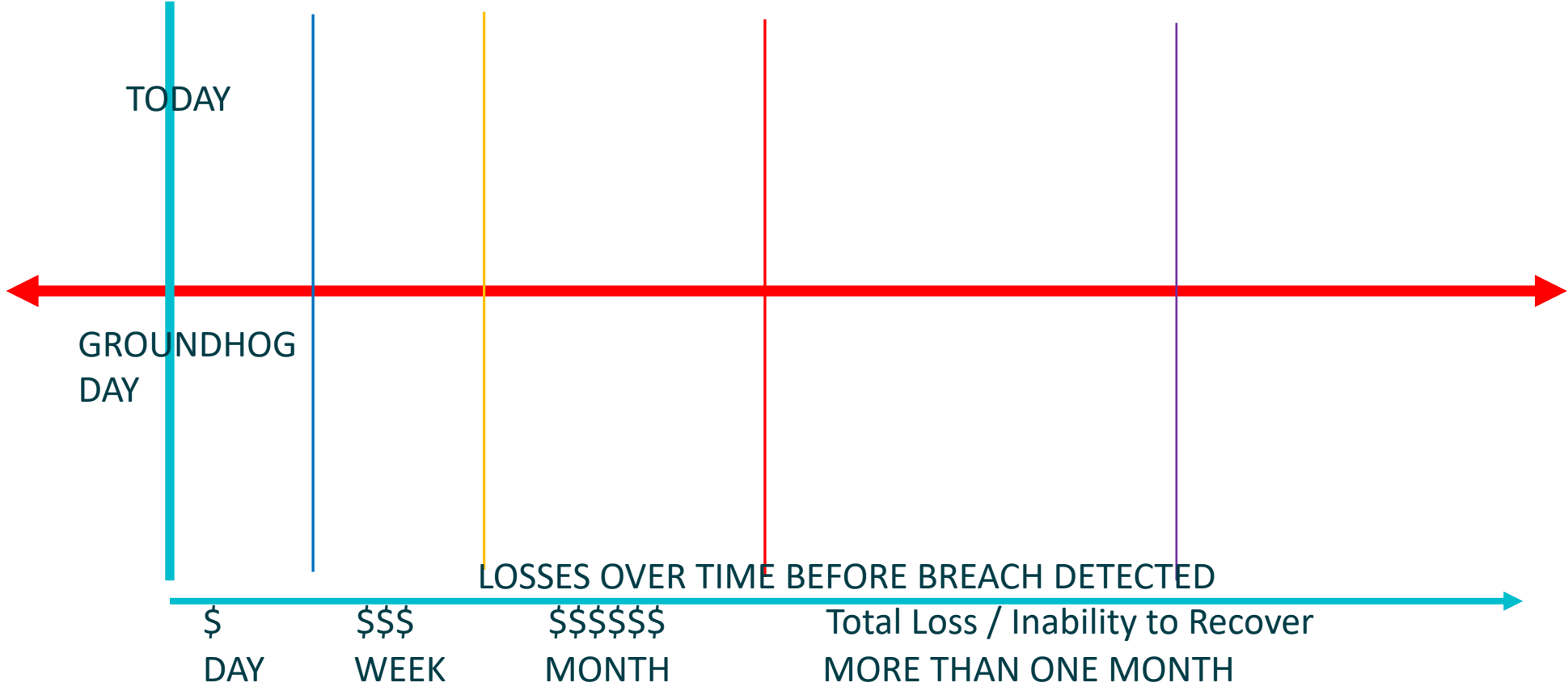
We do not have the luxury of a
Groundhog Day until we get it right

Loss incident means significant
financial, reputational & operational
loss

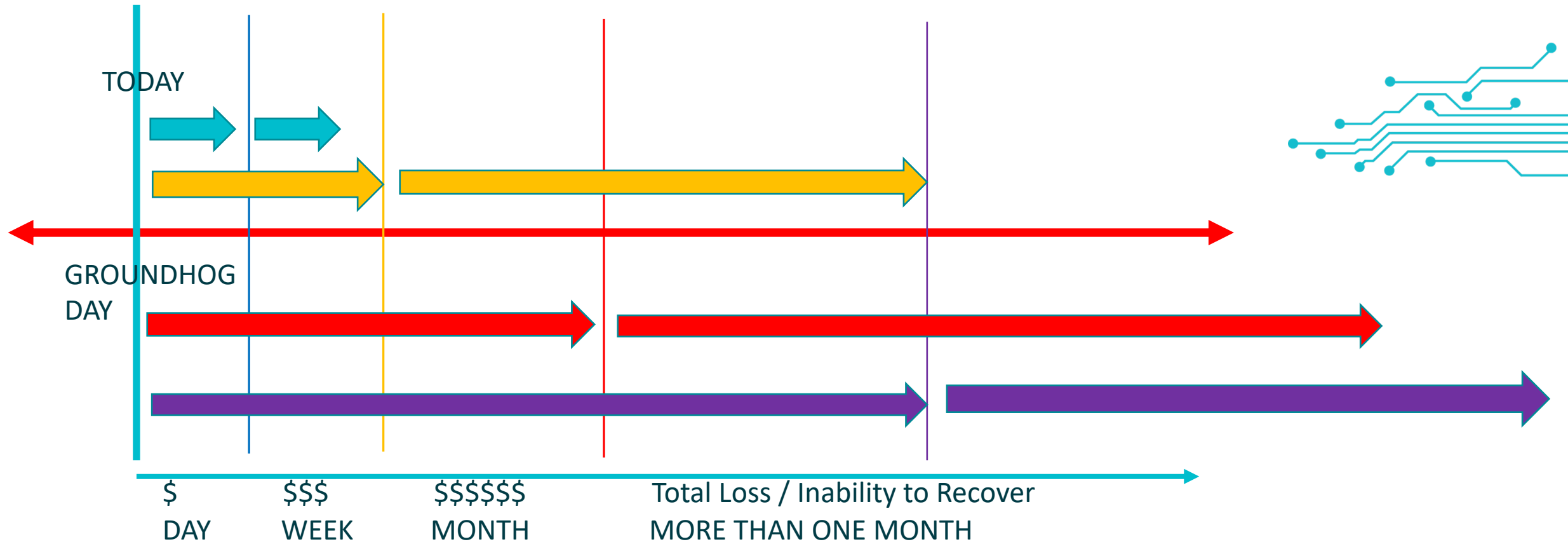
...what happens on the other side of
'today'?



Get closer to 'Today' when bad things happen...



...exponential relationship between detection time & recovery time



Contact us anytime for a
consultation!

tyson.johnson@cybernb.ca

CYBER**NB**

CIP**net**

Critical Infrastructure Protection

