EVERSHEDS SUTHERLAND

Writing a global pandemic playbook – a three part series

Crisis control: Effectively managing teams and protecting organization in the era of COVID-19 cyber attacks and insider threats

May 12, 2020

Michael Bahar
Partner, Eversheds Sutherland - Washington DC

Paula Barrett
Partner, Eversheds Sutherland - London

Dennis Garcia
Assistant General Counsel, Microsoft

ACC Association of Corporate Counsel CHICAGO

Agenda

- The New Normal, including the increased threat environment
- Lawyers as leaders
- Deliberate vs dynamic planning and execution
- Breach response maxims
- Best practices for prevention
- Privacy and security considerations for new technology

The New Normal

Hackers thrive amidst confusion

Bloomberg

Paris Hospitals Target of Failed Cyber-Attack, Authority Says

REUTERS

Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike

FINANCIAL TIMES

Ransom attackers set sights on financial sector 'big game'

Off-the-shelf malware from the dark web is being used to target larger victims and sums

The key threats

Phishing attempts

- Substantial increase in numbers being reported
- Techniques used include bogus emails with links claiming to have important updates
- Originate globally and have led to detrimental financial impact and loss of sensitive data

Malicious sites and apps

- National Cyber Security Centre has been taking measures to automatically discover and remove malicious sites which serve phishing and malware
  - Use “COVID-19” and “Coronavirus” as a lure to make victims click the link or advertise fraudulent treatment products

Attackers posing as a state welfare provider

- Examples of operations where attackers have been distributing infected Word documents. Operations like this have been used in
  - Japan
  - Indonesia
  - The US
  - Italy

The key threats

- **Fundraising scams by fake charities**
  - Solicit donations and purport to be involved in fighting the spread of Coronavirus
- **Investment pump-and-dump scams**
  - Criminals promote penny stocks for companies that claim to have Coronavirus treatment products
- **Registration of new domain names**
  - These contain “Coronavirus” or “COVID-19” wording designed to obfuscate true purpose
- **Fake or misleading corporate information**
  - Information sought to authenticate customers/transactions being faked or amended
- **Unusual account activity**
  - Unusual transactions or volumes as a result of illicit COVID-19 related activity

Lawyers as leaders

Role of in-house and outside counsel

- Whether in deliberate planning or dynamic planning, deliberations or execution, in cybersecurity and IP protection, the role of the lawyer is critical
- It is about anticipating, identifying, managing and mitigation risks – not necessarily eliminating risk
  - Seek to reduce complexity and uncertainty, not add to it
  - Risk may be a function of time
- Lawyers are leaders, especially in crises
  - Lawyers can make the difference between a bad day, and a tragic year

10 Cs Best Practices

Character → Calm → Confidence → Communicate → Clarity → Collaborate → Create → Courage → Change → Compassion

@DennisCGarcia

Deliberate vs dynamic planning and execution

If you have a plan, and the time…

- Consider how the plan applies to a teleworking and reduced workforce
  - Who is the Response Team?
  - Who are the back-ups?
  - Do the back-ups know they are back-ups, and do they know the plan?
  - Can I contact the Team (and their back-ups)?
  - What if my computer and phone go down?
  - Does the situation increase the Insider Threat?
- Ensure the plan is accessible and identify other potential single points of failure

If you have a plan, and the time…

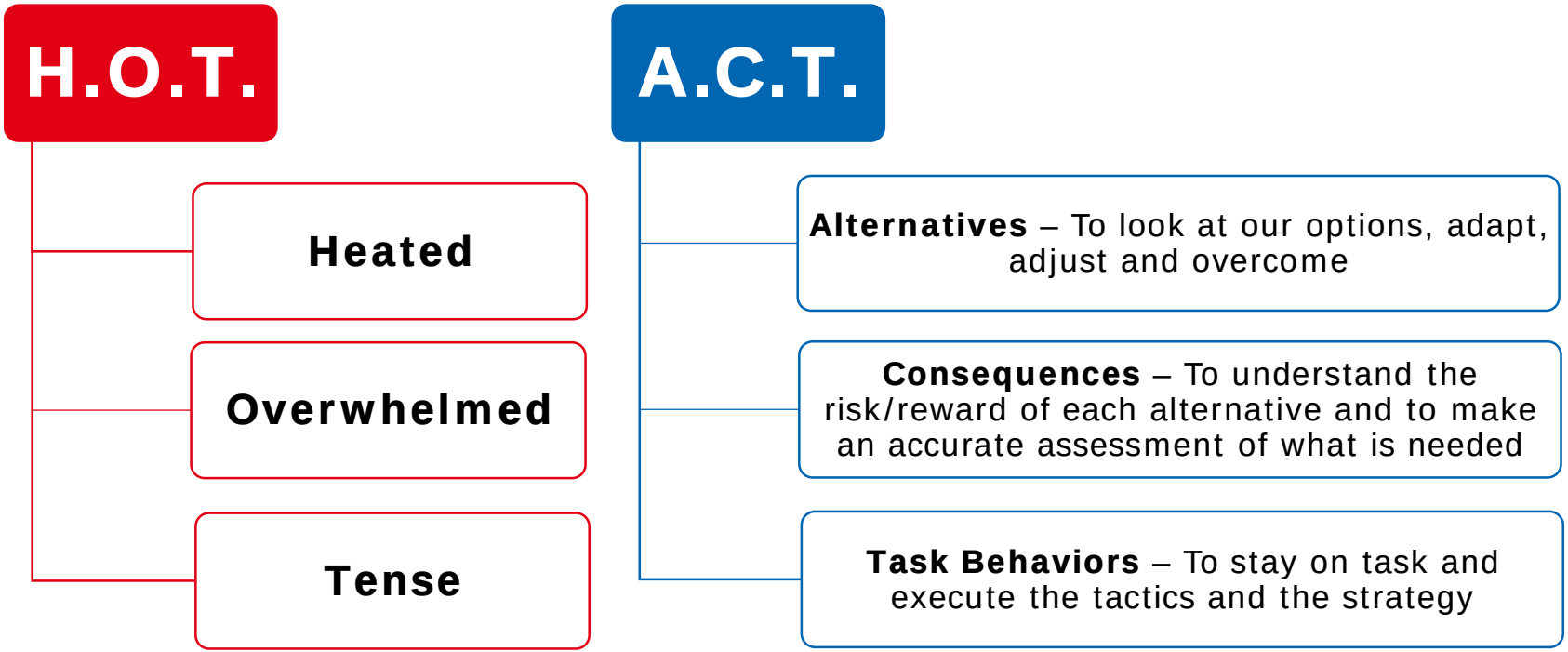
- Deliberate planning
  - Review and understand your regulatory obligations
  - Review and understand your contractual obligations
  - Review your cyber insurance
  - Pre-clear your external advisors and consultants

When time is of the essence…

- In the midst of a crisis, whether a public health emergency, a cyber attack or both, it is important to look up from the plan, adapt to the changed and changing circumstances, and not necessarily try to follow every word of it
- OODA Loop
  - Observe
  - Orient
  - Decide
  - Act
- Everything needs to be coordinated

Dynamic planning and execution

Red Head versus Blue Head



Breach response maxims

Tips for responding to a breach

- **In the first few moments**: take steps to immediately stop the bleeding – do not ignore the problem
- **Breath**: while the clock is ticking, you have time to ACT
- **Look out for Kid Soccer**: this is especially important when teams are apart
- **Notification requirements**: vary by state, and around the world, and not every attack may trigger the notification requirement
- **What to say**: what to say in a notification is as important as whether to notify, especially when it comes to shareholders, regulators and courts

Best practices for prevention

What if I don’t have a plan?

- Now is the time to start
- Don’t worry about being perfect
- Recognize that every little bit helps
- Remember: you don’t have to outrun the bear, only the slowest camper

Prevention best practices you can do now

- Remind employees
  - Beware of phishing – do not click on suspicious links
  - Beware of Information Warfare Attacks
  - Be mindful of personal data/confidential information (even trade secrets) being transmitted or overseen/overheard
  - Smart social media usage
- Remote access
  - Use a secure connection (e.g. VPN)
  - Enable Wi-Fi security features
  - Restrict access control
  - Antivirus software up-to-date
  - Latest versions/patches
- Ensure offsite backups
- Continue employee training

Privacy and security considerations for new technology

As things change, so must we

- Consider cybersecurity and privacy aspects of new means of communication
  - Be deliberate, wherever possible, about implementation and/or adoption
    - What might be acceptable risk in the early days of a crisis, may not be acceptable the longer a new normal sets in
- Consider/manage platforms being used by employees (and those platforms the company considers “preferred”)
- Look at applications being accessed via a public network
  - Does the application have end-to-end encryption?
  - Does the application have a chat history that interferes with an employee’s right to privacy?
  - What about recordings?

EVERSHEDS SUTHERLAND

Michael Bahar
Partner
Eversheds Sutherland – Washington DC
michaelbahar@eversheds-sutherland.com
+1 202 383 0882

Paula Barrett
Partner
Eversheds Sutherland - London
paulabarrett@eversheds-sutherland.com
+44 20 7919 4634

Dennis Garcia
Assistant General Counsel
Microsoft
@DennisCGarcia

eversheds-sutherland.com