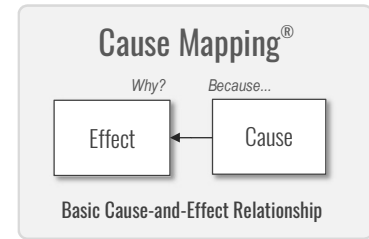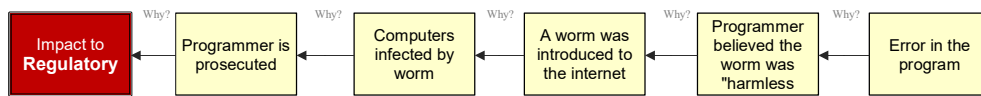# The Morris Worm: The First Significant Cyber Attack

On November 3, 1988, Robert Morris, a graduate student at Cornell, created and released the first computer worm that could spread between computers and copy itself. Morris didn't have malicious intent and his worm appears to have been more the result of intellectual curiosity rather than a purposefully destructive cyber-attack, but an error in the program led to it propagating much faster than he intended. The worm significantly disrupted the young internet, introduced the world to the concept of a software worm and served as a wakeup call on the importance of cybersecurity.
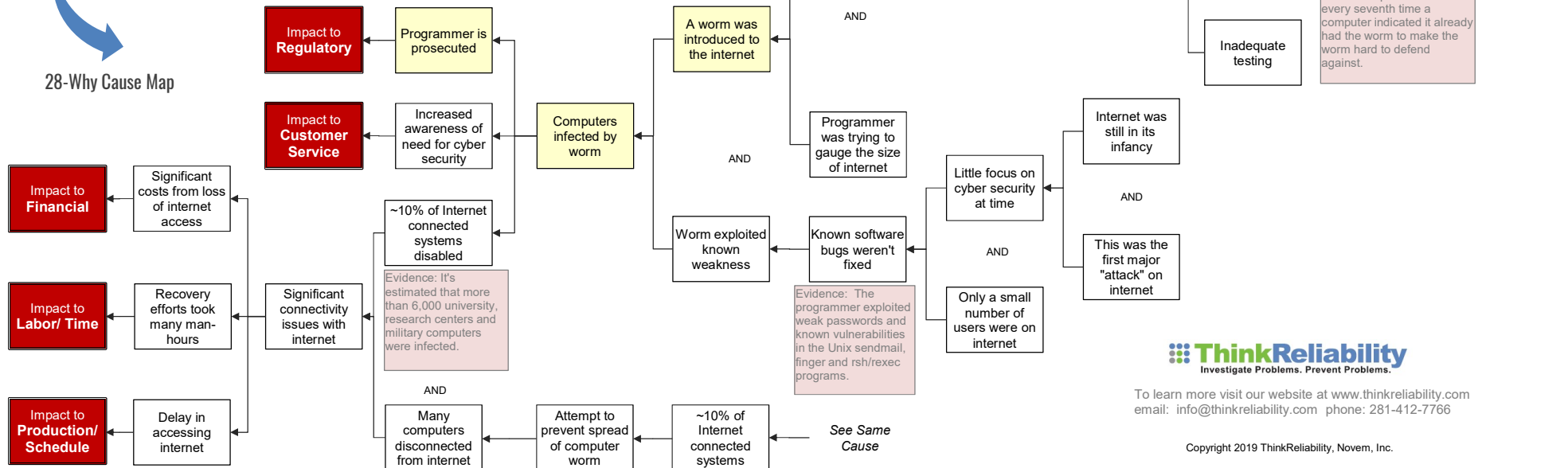
Cause Mapping®

Why? — *Because...*

Effect ← **Cause**

Basic Cause-and-Effect Relationship

Start Simple A Cause Map, or visual root cause analysis, can be used to analyze this issue. A Cause Map is built by asking "why" questions and using the answers to visually lay out the causes that contributed to an issue to intuitively show the cause-and-effect relationships. Start by asking a few why questions.

5-Why Cause Map

Impact to **Regulatory** ←Why?— Programmer is prosecuted ←Why?— Computers infected by worm ←Why?— A worm was introduced to the internet ←Why?— Programmer believed the worm was "harmless" ←Why?— Error in the program

Expand as Needed Continue asking "why" questions to continue adding causes to the Cause Map. Mapping out all the causes that contributed to an issues ensures that all facets of a problem are well understand and helps facilitate the development of effective, detailed solutions that can be implemented to reduce the risk of a similar issues in the future.

28-Why Cause Map

Impact to **Regulatory** ← Programmer is prosecuted

Impact to **Customer Service** ← Increased awareness of need for cyber security ← Computers infected by worm

Impact to **Financial** ← Significant costs from loss of internet access

Impact to **Labor/ Time** ← Recovery efforts took many man-hours ← Significant connectivity issues with internet

Impact to **Production/ Schedule** ← Delay in accessing internet

~10% of Internet connected systems disabled

Evidence: It's estimated that more than 6,000 university, research centers and military computers were infected.

Many computers disconnected from internet ← Attempt to prevent spread of computer worm ← ~10% of Internet connected systems ← *See Same Cause*

A worm was introduced to the internet

Programmer was trying to gauge the size of internet

Worm exploited known weakness ← Known software bugs weren't fixed

Evidence: The programmer exploited weak passwords and known vulnerabilities in the Unix sendmail, finger and rsh/rexec programs.

Little focus on cyber security at time ← Internet was still in its infancy

AND — This was the first major "attack" on internet

Only a small number of users were on internet

Programmer believed the worm was "harmless" ← Programmer didn't intend to disable computers

Evidence: Statement by programmer. Verified by examining the code of the worm.

AND

Worm didn't behave as intended ← Error in the program

Worm quickly re-infected computers over and over ← Programmer underestimated the speed of propagation

AND

Potential reinfection was part of the design ← Intended to make the worm difficult to defend against

Evidence: The programmer wanted one copy of the worm to infect each computer, but designed the worm to duplicate itself every seventh time a computer indicated it already had the worm to make the worm hard to defend against.

AND

Inadequate testing

ThinkReliability
Investigate Problems. Prevent Problems.

To learn more visit our website at www.thinkreliability.com
email: info@thinkreliability.com phone: 281-412-7766

Copyright 2019 ThinkReliability, Novem, Inc.