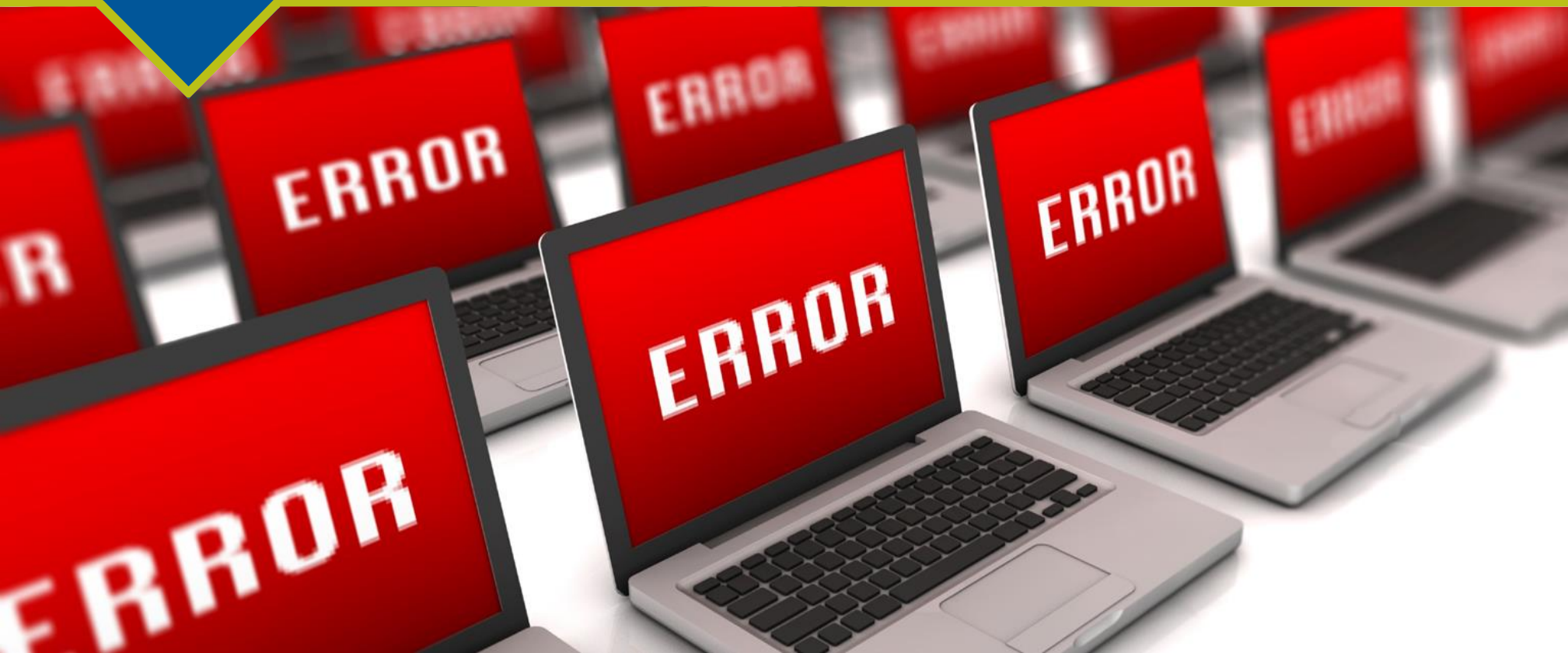




VICTOR D.
SCHINNERER
& COMPANY, INC.

What is Unsupported Software?

Jason Bucher, Senior Underwriting Manager



What is Unsupported Software?

- Why are we talking about this?
- Its just a ploy to sell more software – right?
- Three primary stages to “unsupported software”
- Recent cyber event – and technology industry response
- Policy condition/exclusions that are impacted
- Questions

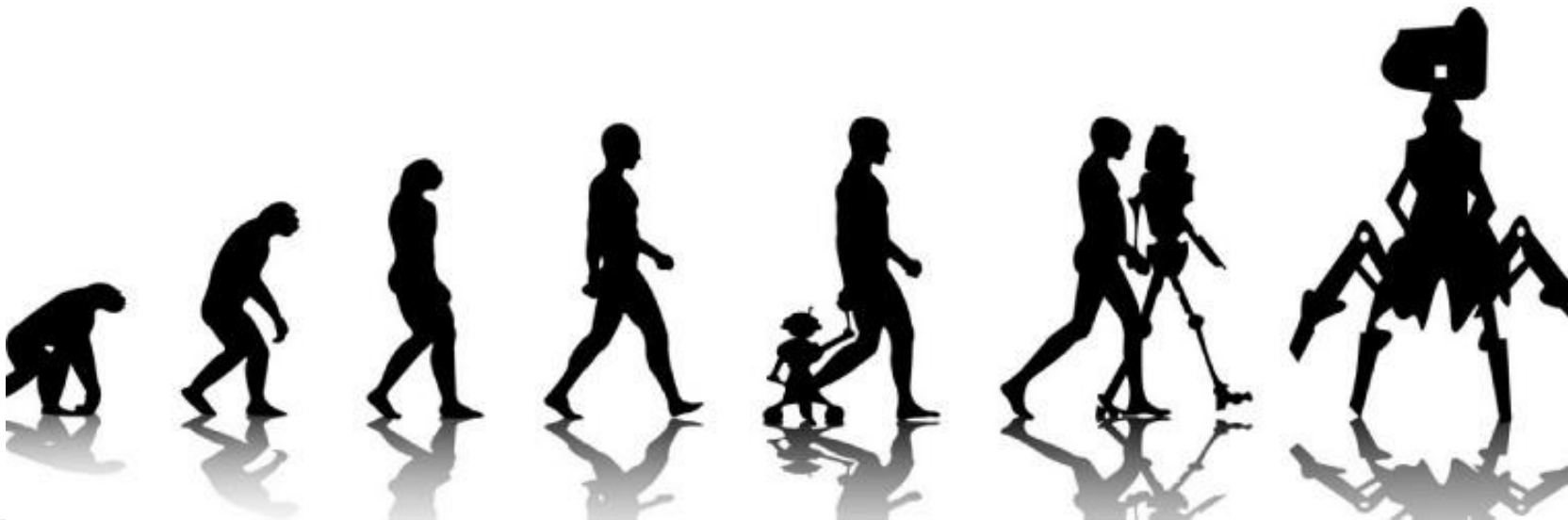
Why Are We Talking About This?

- WannaCry brought the topic and perils of unsupported software to the forefront
- WannaCry exploited vulnerabilities in older operating systems (Windows 7 primarily) in order to both infect and spread
- Many cyber policies carry either an unsupported software exclusion or condition in some form or other – making this an important topic for cyber insurance discussion



Why Are We Talking About This?

- Why would software ever go “unsupported”
 - Rapid evolution of hardware
 - Rapid evolution of software
 - Rapid evolution of user demands/preferences
- All lead to demands that exceed the performance capabilities of the original product



Unsupported Software

- Unsupported Software is complex and often depends on the software itself and the developer
- Three primary stages to Unsupported Software for mass market software packages:
 - End of mainstream support
 - End of extended support
 - Cease of updates for specific platforms



End of Mainstream Support

- Even as bugs are found, it's not going to get fixed unless it poses a security risk
- The software will continue to work, but as non-security issues arise, you have to either live with it or develop in-house workarounds
 - No new Features or product tweaks
 - No free help or support will be provided
- Example: Windows 7 – January 13, 2015
 - Patch for Windows 7 to protect against WannaCry was released March 14, 2017



End of Extended Support

- Even security issues will not receive fixes or patches
- The software will continue to work, but you are on your own and use of software will place you at risk
 - This generally follows a considerable period of “End of Mainstream Support”
- Example: Windows XP – April 8, 2014
 - Unusual step: Microsoft pushed patch to fix Microsoft XP, Windows 8 and Windows Server 2003 against the WannaCry virus threat in May and then this month (June 2017) pushed another batch of security fixes



Cease of Updates to Specific Platforms

- Updates to software product will not work on older platforms
- Allows for targeted product improvement
- Example #1: Internet Explorer – as of January 12, 2016, only the most current version of Internet Explorer (IE 11) will continue to receive updates and fixes
- Example #2: Google Chrome ended support for Windows XP – new versions of Chrome will not work on Windows XP



User Experience with Unsupported Software

- End of mainstream support
 - New software and services will lead to errors or unsteady performance and user experience
 - Patch delivery can involve delays requiring research and testing due to incompatibility with newer software packages
 - Security issues will still receive the attention it deserves from developer
- End of extended support
 - Significant impact to user experience with incompatibility issues abound
 - Significant security risk
- Cease of updates to specific platforms
 - Impact to user experience with incompatibility issues and potential security risk.

Recent Cyber Event – Policy Condition Impact

- WannaCry Virus
 - Designed to exploit a recently discovered vulnerability in Microsoft Software
 - Approximately 98% impacted users were Windows 7 users
 - All impacted Windows 7 users did not have recent updates/patch
 - Use of “Unsupported Software” often leads to delay in implementation of patches and can lead to accelerated distribution in the community.
 - Exclusion or condition limiting coverage for “Use of Unsupported Software”



Cyber Exclusion/Condition Impact Continued

- The term “Unsupported Software” is generally not defined in an insurance policy
- Many policies carry this coverage condition (be sure to discuss and evaluate with clients)
- Schinnerer Cyber Protection Package does not have this coverage condition or exclusion



CYBER PROTECTION PACKAGE

CYBER RISK
Cyber attacks are escalating in frequency and intensity, and pose a growing threat to the business community. Many recent incidents reflect the expanding spectrum of cyber threats — from hackers stealing customer account information, to attacks meant to disable a company's website. Companies in greater numbers are seeking financial protection through skillfully underwritten cyber liability coverage.

TARGET MARKETS
Any small and mid-size organization that utilizes electronic systems

THE SPECS
AVAILABILITY: In 47 states and D.C.*
MINIMUM PREMIUM: \$750
LIMIT: Up to \$10 million
COVERAGE: Admitted with an A rated carrier
* state filings pending in FL, NY and WA

BREACH RESPONSE TEAM
The cyber breach response team associated with the Schinnerer Cyber Protection Package provides expert legal services and technical support designed to assist policyholders who have identified a data security breach.

- Breach response capabilities including forensics, legal advice, etc.
- Risk management tools that decrease your exposure as well as provide industry-specific guidance

COVERAGE BUNDLES & OPTIONAL ENDORSEMENTS

DIGITAL CRIME:
First-of-its-kind bundle of coverages to protect your company from various types of digital crime including:

- Electronic transfer of funds
- Cyber extortion
- Telephone toll fraud
- Deceptive transfer

BREACH LIABILITY:
Broad liability coverage for any suits or demands related to cyber that result in a loss to your company including:

- Privacy liability
- Payment card industry
- Website media liability
- Regulatory

BREACH RECTIFICATION:
Coverage designed to get your business back on track as quickly as possible all while protecting your company's brand and reputation. The coverage suite includes:

- Data breach team
- Digital asset loss
- Business interruption

SUBJECT MATTER EXPERT
Jason Bucher
Jason.Bucher@Schinnerer.com
(913) 685-6166

WEBSITE
www.Schinnerer.com/Cyber

Victor O. Schinnerer & Co., Inc. | Two Wisconsin Circle | Chevy Chase, MD 20815
Phone: 301-961-9800 | Fax: 301-951-5444 | www.schinnerer.com | vos.info@schinnerer.com
This information is for illustrative purposes only and is not a contract. It is intended to provide a general overview of the policy described.
Nothing contained herein should be construed as an acknowledgment by Schinnerer that a given situation may be covered under a particular policy.
© 2015 Victor O. Schinnerer & Company, Inc. | In CA, dba Schinnerer Insurance Services | CA Ins. Lic. # 0156109

Cyber Protection Package Resources

Data Response Team

Your Schinnerer Cyber underwriters



Jason Bucher



Mark Schulz



Denise Mahoney

Contact Us



Jason Bucher

Senior Underwriter

Phone: (913) 685-6166

jason.bucher@schinnerer.com



Matt Kletzli

Management Liability Leader

Phone: (301) 961-9820

Matthew.Kletzli@Schinnerer.com



VICTOR O.
SCHINNERER
& COMPANY, INC.