# TODAY'S CYBER LIABILITY LANDSCAPE

2017 brought another year of increased cyber security incidents. Headline breaches have business leaders wondering what's next. In an ever increasing online world with a confusing abundance of cyber security strategies and sterner regulations, both domestically and internationally, criminal cyber activity shows no signs of slowing down.

## WHAT TO WATCH FOR:

1. Cyber activity will not only continue to dominate in the core industries handling valuable data (financial, retail, and healthcare) but will expand in other areas, such as governmental and educational entities.
2. Ransomware attacks, like the major global WannaCry attack of 2017, will rise. Targeted, individual organizational attacks will continue but widespread global attacks will increase in frequency as well.
3. The rise in the acceptance and value of different cryptocurrencies (i.e. Bitcoin) will allow cyber criminals to engage in activity with untraceable transactions and make cybercrime even more attractive.
4. Financial institutions will see increased cyber incidents. Consumer demand for real-time cross-institution transactions will make speed, not integrity, the competitive goal. In addition, ATM-compromising malware is flooding the market.
5. Regulatory pressure is reaching boiling point. 2017 was very active in regard to U.S. State regulator investigations and issued fines. Though many federal agencies are vying for oversight of cyber security, there is no federal legislation on the horizon. It will remain a state issue.
6. European Union's (EU) General Data Protection Regulation (set to launch May 25, 2018) applies to all organizations that interact with EU residents. This will set a major precedent for federal entity regulation of global security.
7. Cyber claims against C-Suite executives will continue to rise. Cyber security must be prioritized as a boardroom concern.
8. Cloud-based service solutions provide efficiencies but can come at a security cost. It's critical to manage contractual risk with third party vendors; breaches are the responsibility of the entity that owns the data.

## 2017 FACTS & FIGURES

**$60T**
Estimated annual cybercrime damages by 2021

**$3.62M**
current average cost of a data breach

**1,300**
Domestically reported data breaches
(Up from 1,093 in 2016)

**WANNACRY** affected:
**300K** organizations in
**150** countries in
**2** days

**4,000+** ransomware attacks have occurred every day since the beginning of 2016 (Kaspersky)

**Three largest root causes of breaches:**

- Malicious/Criminal Attack (47%)
- Human Error (28%)
- System Glitch (25%)

FREEDOM TO MOVE FORWARD

Madison | Milwaukee | Green Bay | Wausau | Eau Claire **800.272.2443 | m3ins.com**

M3 INSURANCE