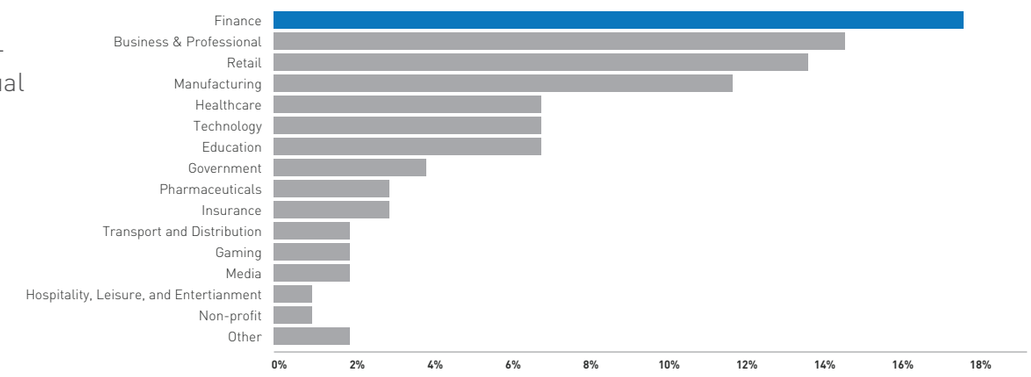
CYBERSECURITY & THE FINANCIAL SERVICES SECTOR

THE NEXTWARE SESSIONS

The financial services sector includes a broad range of businesses from local credit unions to trillion dollar investment firms. The Department of Homeland Security (DHS) identifies the sector as critical infrastructure, which includes the "assets, systems, and networks...so vital...that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." As seen in the chart on the right, the financial sector experiences some of the highest annual cyber incident rates.

"What is most interesting about the financial markets is that they are so demonstrably interconnected, and therefore an effect felt in one market might quickly spread to interconnected markets and organizations."
—Computer Weekly

ATTACKS BY SECTOR 2014
—NTT Group, 2015 Global Threat Intelligence Report



THE CYBER THREAT

ATTACKS

"While security technologies and user awareness are improving, malicious cyber activity is likely to continue in the future. Even more concerning is the prospect of a more destructive incident that could impair financial sector operations."
—Financial Stability Oversight Council Report, 2015

Attacks range from small-to large-scale attacks designed to achieve a variety of objectives.

ATTACKERS

Attackers range from rogue insiders or cyber criminals to well-resourced networks or nation states with complex political and economic motives.

INDIVIDUAL OR INSIDER

HACKTIVIST

ORGANIZED CRIME SYNDICATE

TERRORIST ORGANIZATION

NATION STATE OR STATE-SPONSORED ACTOR

IMPACT

SNAPSHOTS FROM 2014

$12.97m

The average annual cost of cyber crime for firms in the financial services sector is $12.97 million.
—Ponemon Institute, 2014 Global Report on the Cost of Cyber Crime

141%

"The number of financial firms reporting losses of $10 million to $19.9 million increased by a head-turning 141% over last year."
—PricewaterhouseCoopers, Global State of Information Security Survey 2015

80 million

80 million identities were exposed by financial sector data breaches.
—Symantec, 2015 Internet Security Threat Report

ATTACK EXAMPLES

DDoS attacks against U.S. banks: 2012-2013

- Izz as-Din al-Qassam Cyber Fighters, with suspected support from Iran, claimed responsibility for major disruptions to online sites of top U.S. banks. The distributed denial of service attacks began in 2012 and continued into 2013.

J.P. Morgan Chase & Co.: discovered August 2014

- Suspected Russian hackers compromised contact information for about 76 million households and 7 million small businesses.

Carbanak cyber crime attacks: discovered February 2015

- Over a period of two years, a multinational cyber criminal gang infiltrated more than 100 banks across 30 countries and stole up to one billion dollars.
- "This is likely the most sophisticated attack the world has seen to date in terms of the tactics and methods that cybercriminals have used to remain covert."—Chris Doggett, Kaspersky North America

CYBER DEFENSE & COLLABORATORS

"The financial sector has historically led the war in making huge investments not only in security infrastructure and the best-qualified people to maintain the systems, but also in driving collaboration across industries and with the government."
—John Carlson, Chief of Staff, FS-ISAC

FINANCIAL SECTOR: AVERAGE ANNUAL INFORMATION SECURITY BUDGET (2014):
—PricewaterhouseCoopers, Global State of Information Security Survey 2015

SMALL ORG
$0.6M -OR- **14.7%** OF IT BUDGET

MEDIUM ORG
$2.6M -OR- **3.3%** OF IT BUDGET

LARGE ORG
$11.3M -OR- **3.7%** OF IT BUDGET

"FINANCIAL-SERVICES COMPANIES PLAN TO BOLSTER THEIR CYBERSECURITY BUDGETS BY ABOUT $2 BILLION OVER THE NEXT TWO YEARS."
– THE WALL STREET JOURNAL

Financial institutions actively engage with public, private, and regulatory agencies in order to address cybersecurity challenges. They share information about threats, vulnerabilities, and incidents affecting the financial services sector.

COLLABORATORS:

DEPARTMENT OF HOMELAND SECURITY

DEPARTMENT OF THE TREASURY

DEPARTMENT OF JUSTICE

U.S. SECRET SERVICE

FEDERAL BUREAU OF INVESTIGATION

INTELLIGENCE COMMUNITY

US-CERT

FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER (FS-ISAC)

REGULATORY AGENCIES:

COMMODITY FUTURES TRADING COMMISSION (CFTC)

CONSUMER FINANCIAL PROTECTION BUREAU (CFPB)

FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)

THE FEDERAL RESERVE BOARD

FINANCIAL INDUSTRY REGULATORY AUTHORITY (FINRA)

OFFICE OF THE COMPTROLLER OF THE CURRENCY (OCC)

SECURITIES EXCHANGE COMMISSION (SEC)

INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (IOSCO)

CONTINUING CYBER CHALLENGES

"A growing challenge facing financial institutions today is the need for greater coordination and harmonization among the regulatory agencies, within the US and globally, to keep pace with new threats, new financial business process models, and the necessary skill sets to evaluate the intersection of those two for security and resiliency purposes." – John Carlson, Chief of Staff , FS-ISAC

"American Express Chairman and CEO Kenneth Chenault said the government needs to aggressively share security information with the private sector and give companies more incentives to share what they know about the issue with one another. "We source over 100,000 attack indicators yearly from various sources, but only 5% come from industry sharing through our ISAC and less than 1% come from the government," he said at the time.—The Wall Street Journal

Center for a New American Security