The $$ of Poor SW Quality

In the US: A 2020 Report

Herb Krasner
hkrasner@utexas.edu
Date: January 27, 2021

CISQ
Consortium for Information & Software Quality™

Abbreviations Used

- CPSQ = Cost of Poor Software Quality
- B = billion
- T = trillion
- US = United States of America
- LOC = lines of code
- SW = software
- OSS = Open Source SW
- FP = function point *(another measure of SW size)*

Introduction to the report

- **Purpose:** to inform and inspire our readers to seek CPSQ knowledge within their own organizations
- **Method:** a unique analysis, synthesis and extrapolation of 88 existing sources of available online information, mixed with some expert knowledge about software and its quality
  - Builds on the 2018 report– basic definitions there –> what is SW quality, Cost of SW Quality model, good vs poor SW quality
- **Result:** a 1st order approximation of the magnitude of this huge and somewhat unrecognized problem

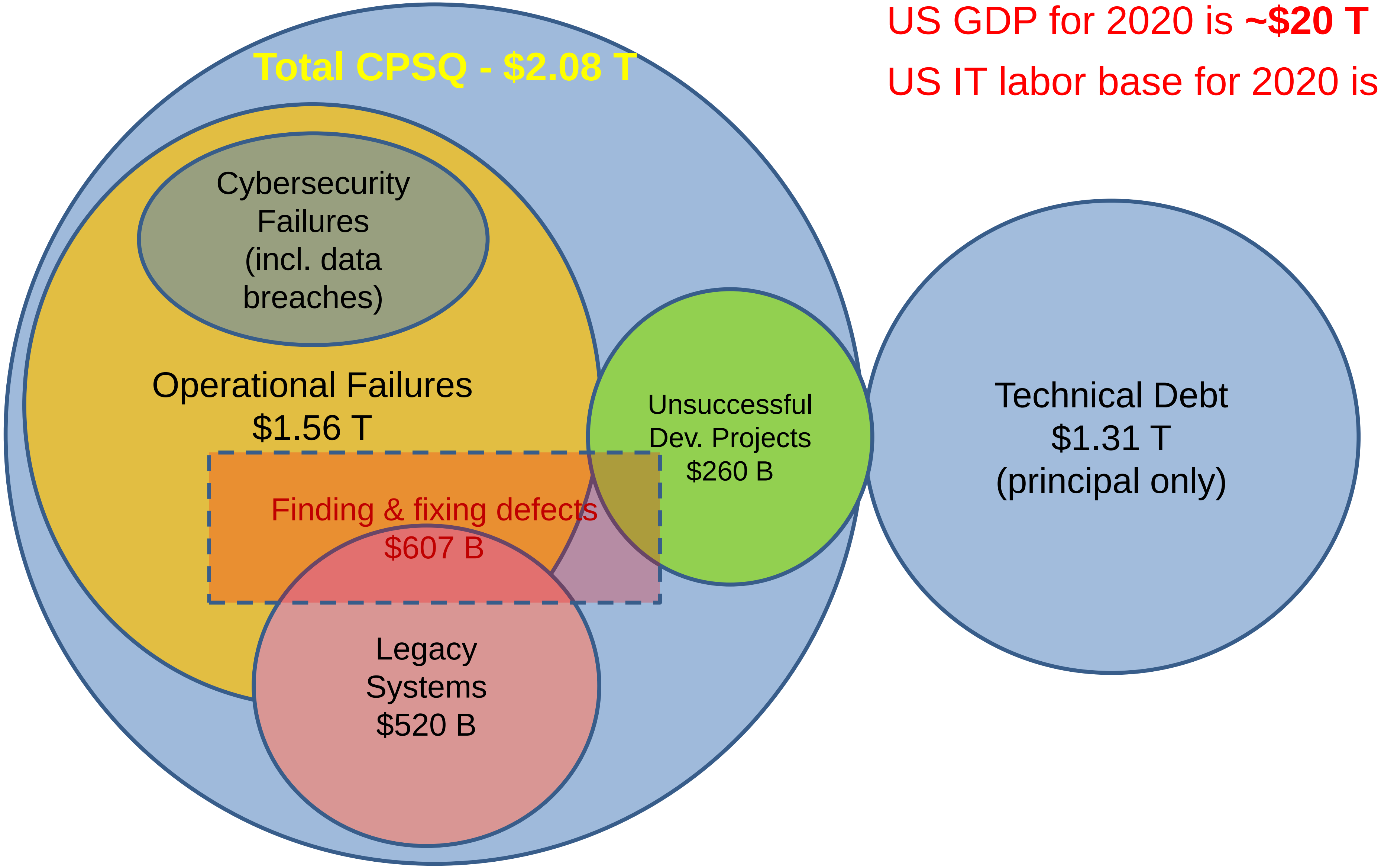
Iceberg Model of CPSQ

Hidden Costs = 6 to 50 times Observable Costs

Summary of Cost Estimates

US GDP for 2020 is **~$20 T**

US IT labor base for 2020 is **~$1.4 T**



Operational Failures: $1.56 Trillion

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach

July 22, 2019

Settlement includes fund to help consumers recover from data breach

Share This Page

result of the 2017 data breach. Equifax will add up to $125

and identity theft services

The Tricentis Software Fail Watch, 5th Ed. reported 606 major software failures from 2017, causing a total loss of $1.7 trillion in assets at 314 companies.
This averages out to $2.8 billion per failure.

WSJ PRO

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

https://www.wsj.com/articles/high-profile-hacks-spark-calls-for-global-cyber-response-11611570601

High-Profile Hacks Spark Calls for Global Cyber Response

Attacks on health-care facilities and government suppliers show need for international response

Microsoft President Brad Smith said the SolarWinds hack was a 'moment of reckoning' that demanded a global response.

PHOTO: BRONTE WITTPENN/BLOOMBERG NEWS

By James Rundle

Jan. 25, 2021 5:30 am ET | WSJ PRO

The challenges posed by modern cyber threats require international cooperation to solve, analysts and lawmakers say, but figuring out how to do that is the hard part.

The cyberattack on SolarWinds Corp. , ransomware gangs targeting health-care facilities, and the global nature of cybercrime have prompted calls from executives and politicians for a global response to cybersecurity problems.

Agreeing on the basic definitions for hostile nation-state action and lesser, criminal activity is the first step, said Scott Crawford, information security research head for the 451 Research unit of S&P Global Inc.'s Global Market Intelligence business.

Failure causality: software flaws

Trends that magnify the impact of software flaws, driving failure costs up:

- 100+ billion new LOC produced worldwide each year -> 25 bugs per 1000 LOC injected on average
- 96 zettabytes of digital data now stored (up from 16 in 2016)
- Growth of cybercrime – ransomware in US cost $9B; $20B worldwide in 2021
- Increasing Digital Transformation: spreading the effects of a software malfunction across the entire value chain.
- Growth of Systems of Systems: expanding complexity exponentially and concealing the triggers for huge failures in a thicket of cross-system interactions.
- Increased Competition: especially online, has prioritized speed-to-business over operational risk and corrective maintenance costs, a huge gamble for systems not designed to expect and manage failures.

Broad Recommendations:

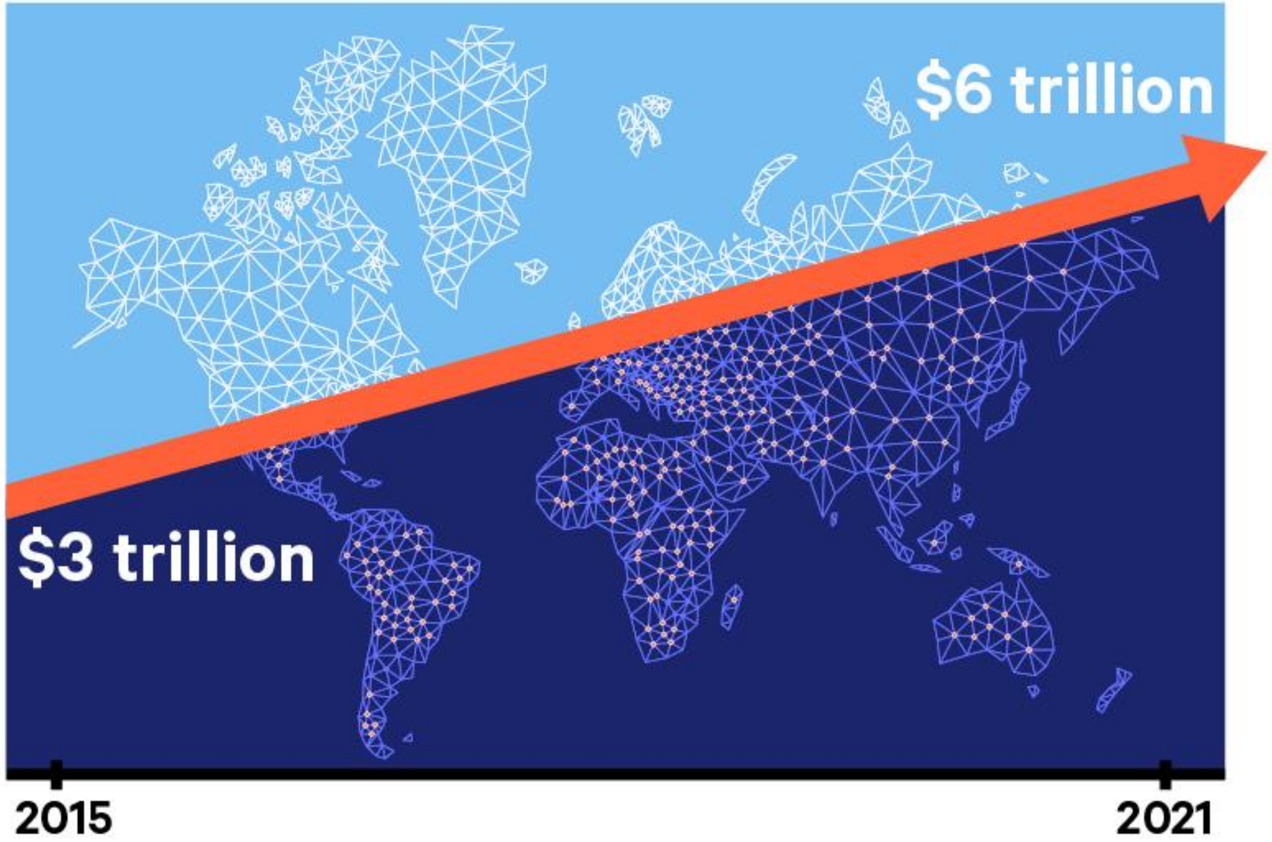
- Prevent bugs, flaws, weaknesses, vulnerabilities from being created and fielded
- Find and fix bugs early
- Measure quality
- Adopt high quality development practices
- Analyze potentially flawed components (e.g. OSS)

1 zettabyte is equal to 1 trillion gigabytes

Cybercrime losses increasing

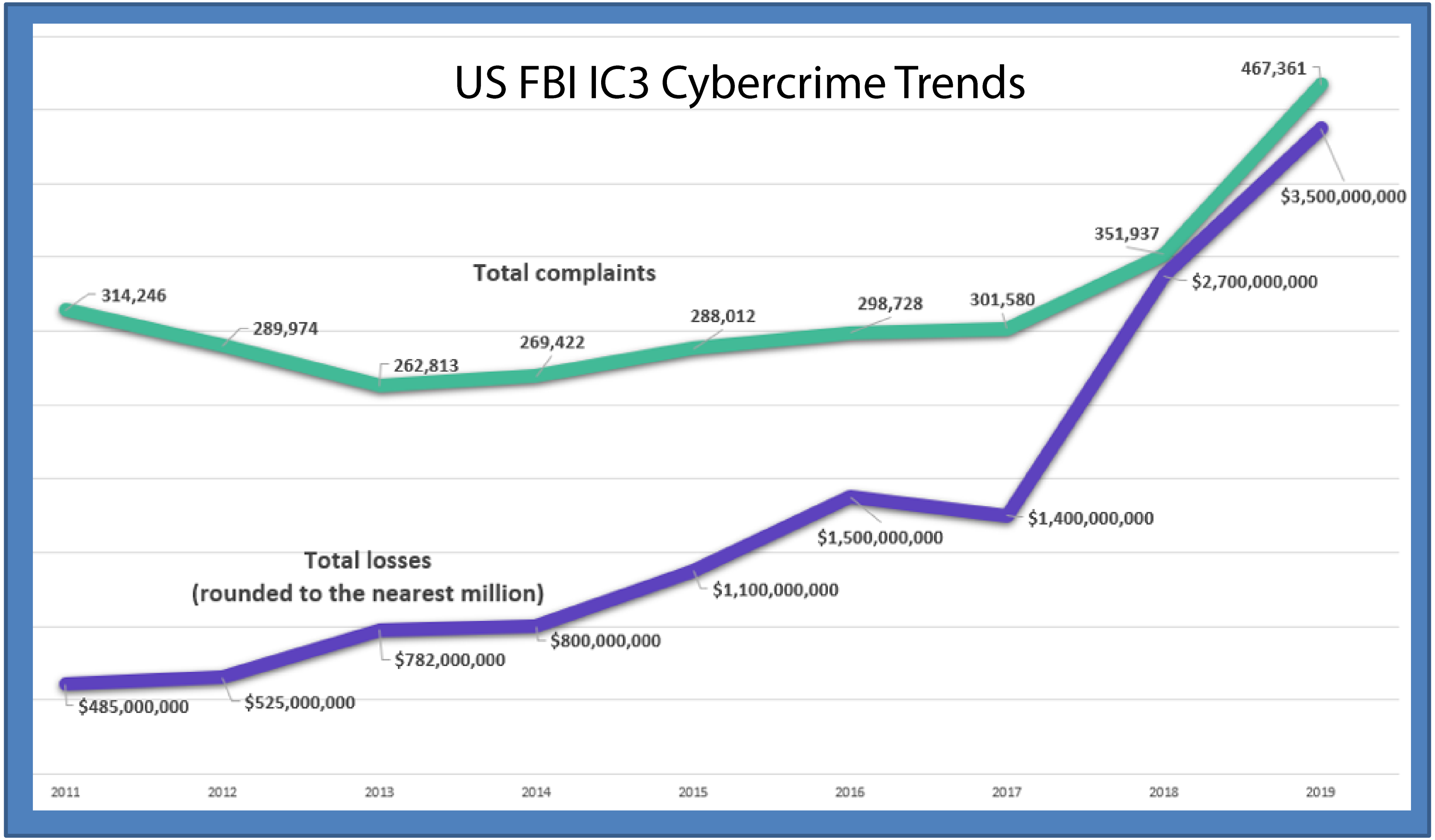
Cybercrime will cost companies worldwide an estimated $6 trillion annually by 2021, up from $3 trillion in 2015.

This is the greatest transfer of economic wealth in history.[1]



1. Embroker, 11/20/2020

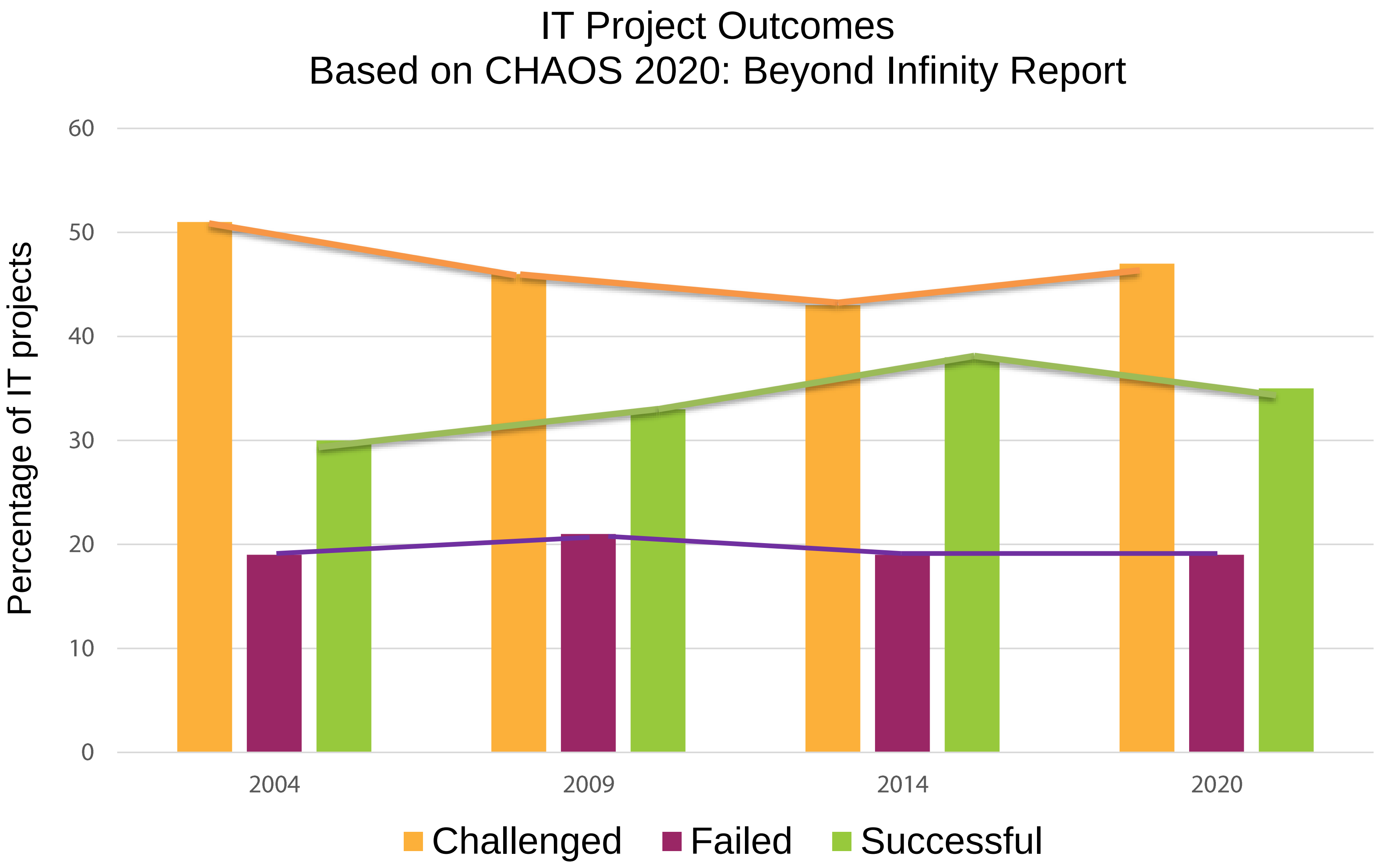
Cybercrime losses increasing



1. Embroker, 11/20/2020

IC3 – Internet Crime Complaint Center

Unsuccessful Projects: $260 Billion



Reduce # of unsuccessful projects

- For projects of large size (10^4 FPs) and above, low-quality projects are 5-6X more likely to be cancelled then high-quality projects.
- Project cancellation rates by size and quality level[1]

1 FP = ~ 100 LOC

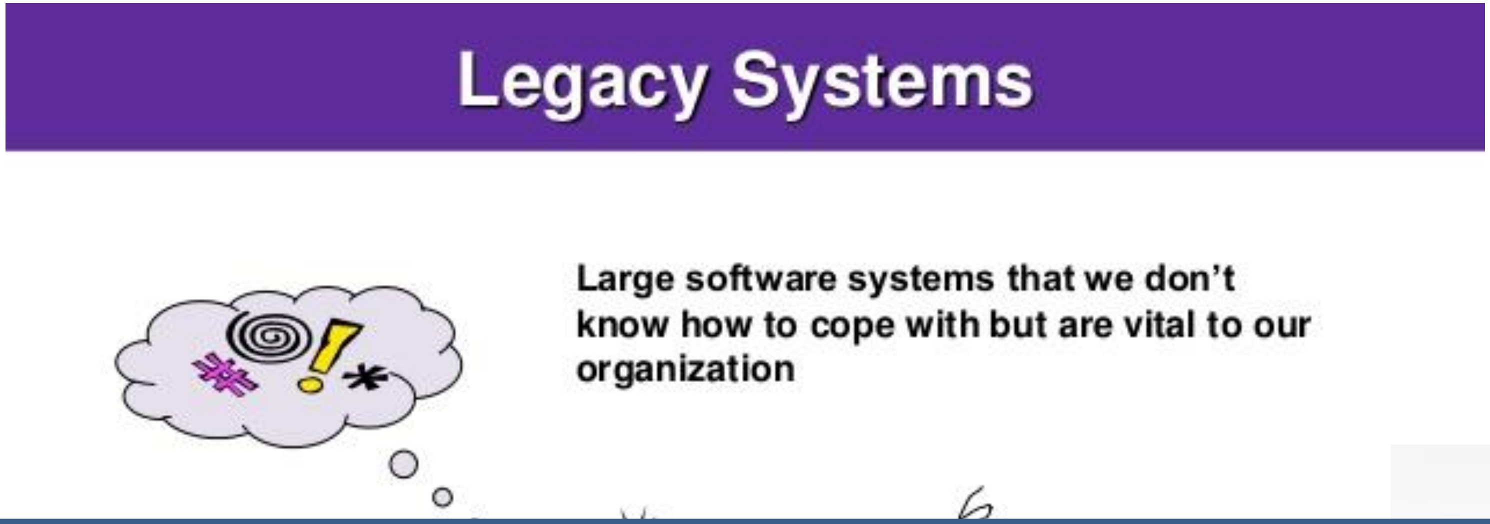
Function Points	High Quality	Low Quality	X-factor
100	.02	.07	3.3
1000	.05	.16	3.2
10^4	.07	.45	6.4
10^5	.12	.65	5.4

Broad recommendations:

- define what quality means for a specific project and then focus on achieving measurable results against stated quality objectives
- use known best practices & tools for achieving high quality
- don't compromise quality for speed to operation

1. Jones and Bonsignor, 2012

Legacy Systems: $520 Billion



Problem: after decades of operation, they may have become less efficient, less secure, brittle, incompatible with newer technologies and systems, and more difficult to support due to loss of knowledge and/or increased complexity or loss of vendor support.

- 70-75% of the IT budget
- 80% of the cost of ownership
- Slight decline in CPSQ due to shifting priorities, work force losses

Legacy systems: broad recommendations

Modernization is not always straightforward. The approach depends on the priority of problems to be solved – functionality, performance, obsolete technology, inflexible architecture.

Several strategies are available to improve CPSQ and COO going forward:

- Encapsulate - to hide/isolate deta
- Rehost – to move systems off the
  the cloud
- Replatform - to speed up with new
- Repair – to fix the bugs, maintain
- Refactor - to reduce technical deb
- Rearchitect - to adapt to a new pla
- Rebuild – to fine tune it
- Replace – with new or SaaS solut

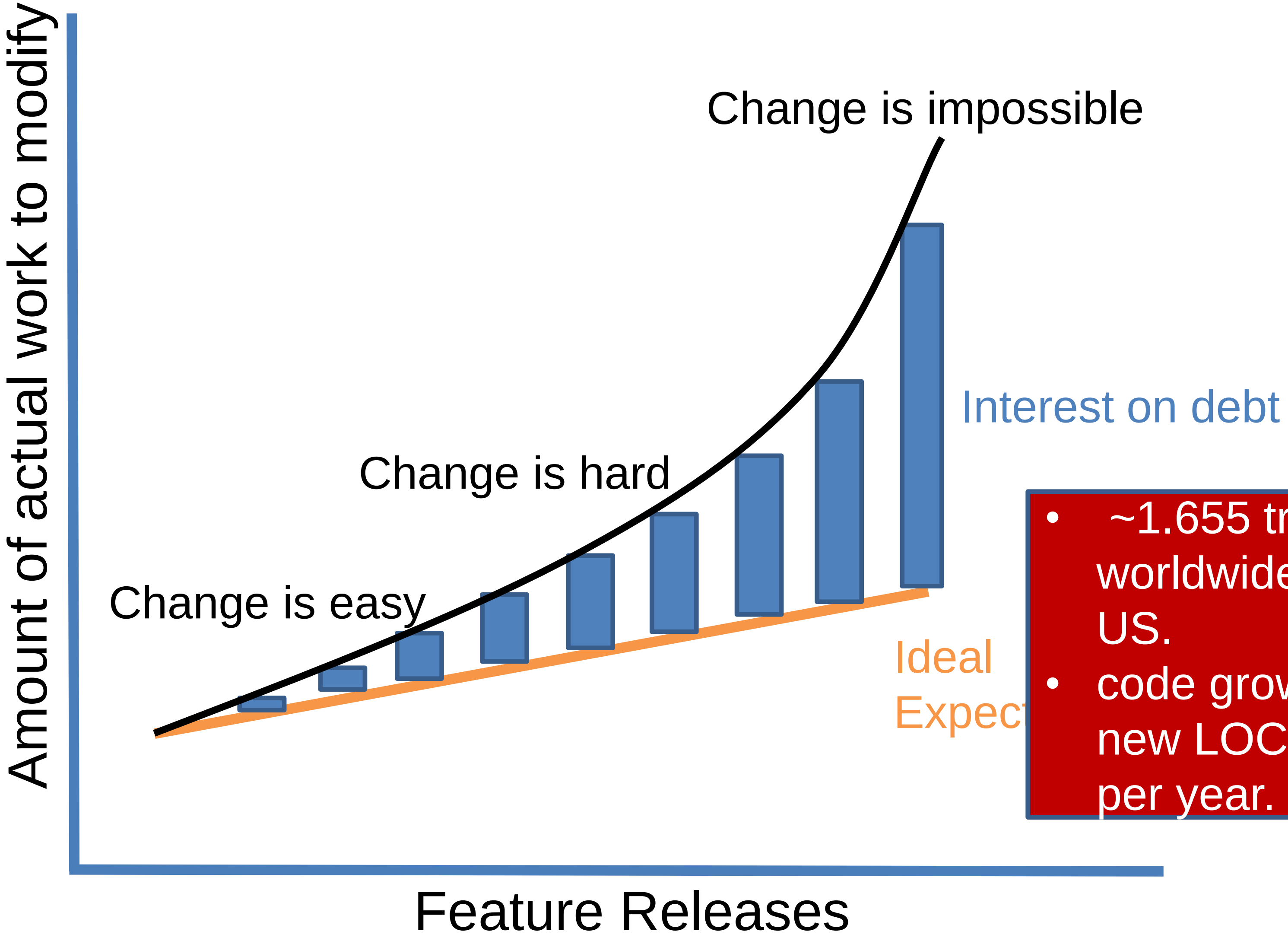
- All these strategies are enabled by overcoming the lack of understanding and knowledge of how the system works internally.
- Any tool which helps identify weaknesses, vulnerabilities, failure symptoms, defects and improvement targets is useful
- Benchmarking the health status of a legacy system is a good starting point.
- Detailed blueprints of system connectivity are useful for modernizing architectures that have degraded over time.

Finding and Fixing Bugs: $607 B

	1	Find, record and prioritize
$	2	Replicate and create a test case
$$	3	Determine root cause
	4	Develop and fix
	5	Try to break the fix
	6	Prove the fix works
$$$	7	Repeat steps 2-6 as needed until done
	8	Record the fix details
	9	Distribute the fix as needed

<u>Prevent first</u> then focus on where the $$$ are spent in the above process to reduce CPSQ and improve productivity

Technical Debt: $1.31 Trillion + Interest

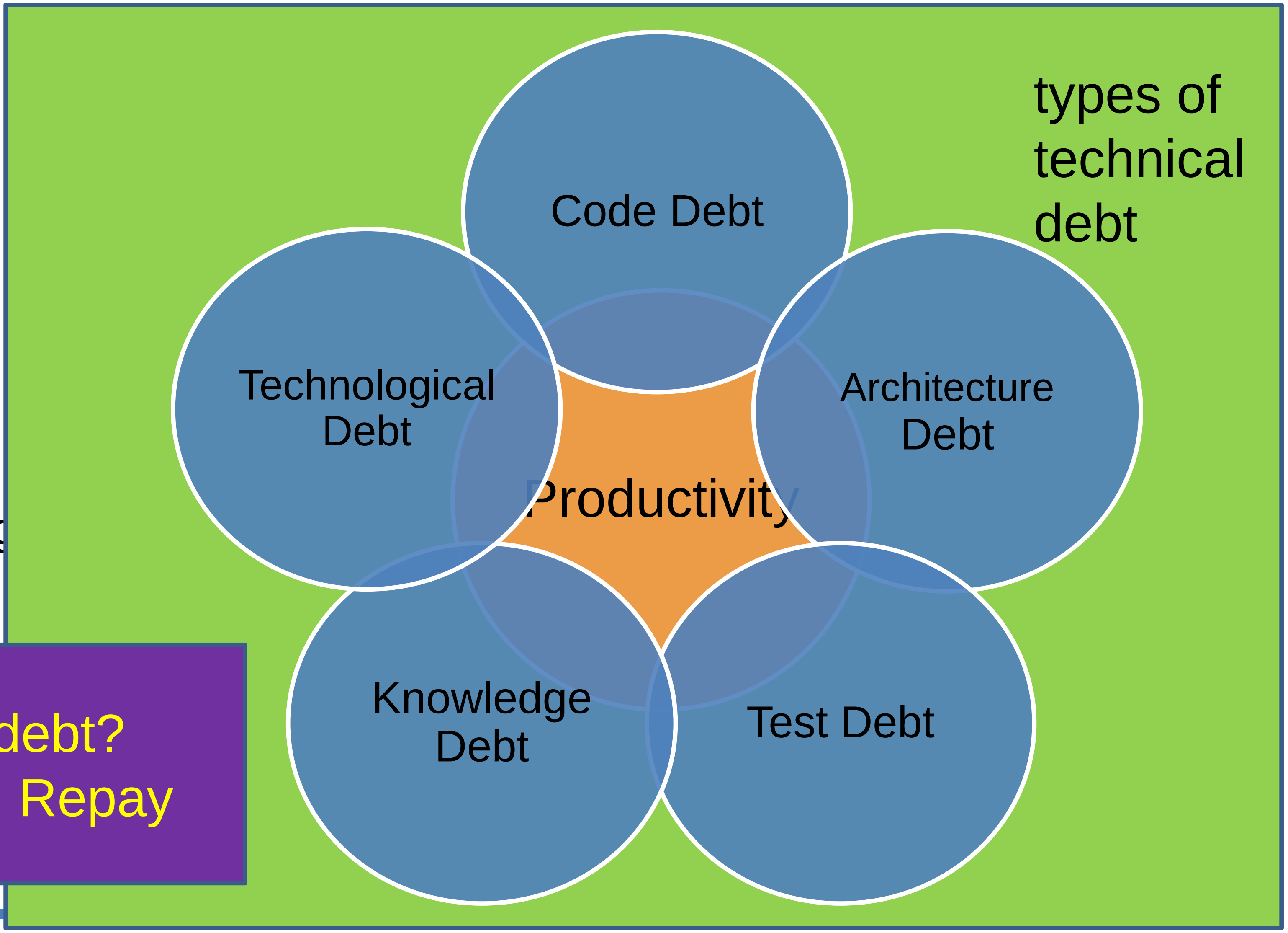


- ~1.655 trillion LOC exists worldwide and 513 billion in the US.
- code growth is now ~100 billion new LOC per year, or ~7% growth per year.

Technical Debt: $1.31 Trillion + Interest

of actual work to modify

Chang



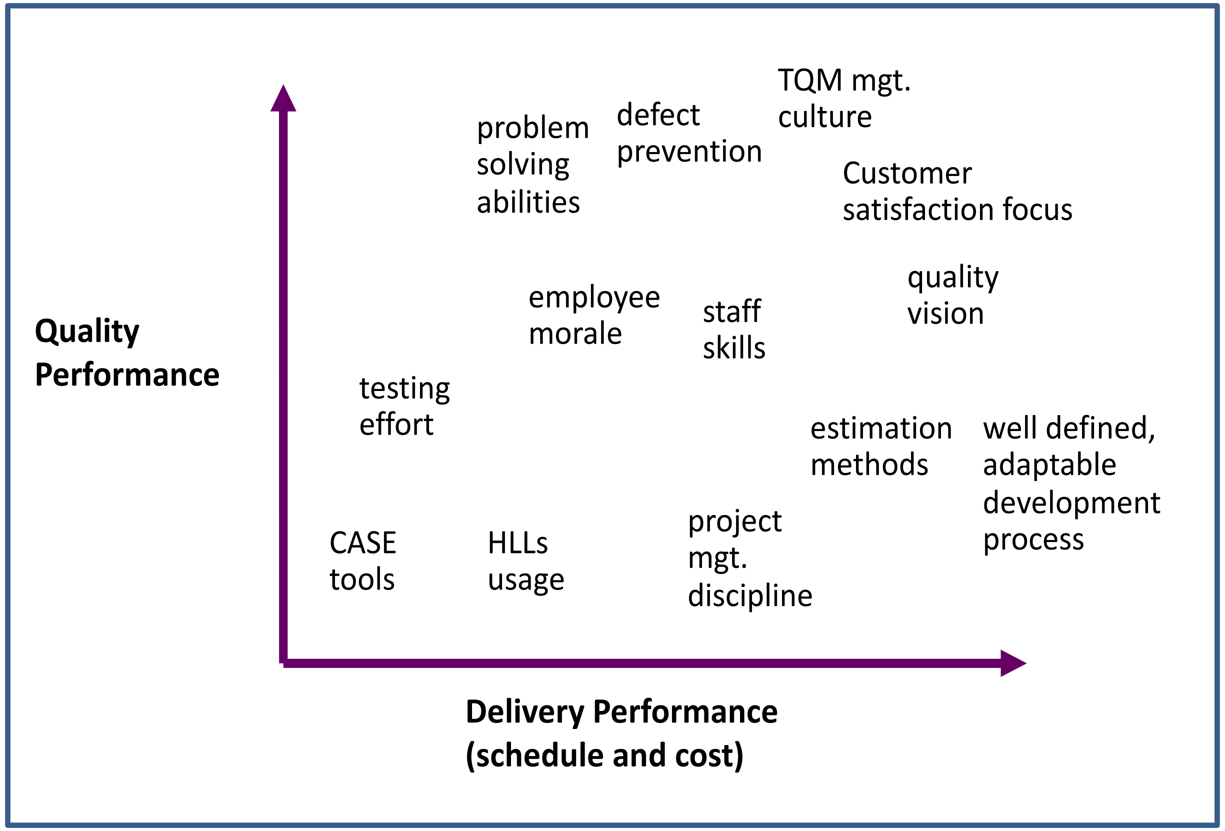
How do you manage technical debt?

- Understand, Elevate, Repair, Repay

Feature Releases

IBM study[1] of 363 EU SW organizations

Performance Factor	Top 10%	Bottom 10%
Productivity (FPs/mo.)	25	5
Delivered quality (% defects removed)	>95%	<50%
Cost/Schedule Performance	<= 10%	>40% over
Post delivery maintenance costs (within 1st yr.)	<1% (of total dev. effort)	>10%



different behaviors

1. derived from: Goodhew, 1996, *Achieving Real Improvements In Performance From SPI Initiatives*, the European SEPG Conference, June 26, 1996.

Broad recommendations in summary

Leaders/C-Suite level
- Establish quality as a 1st-class citizen -> security+
- Ask better questions: externally and internally
- Measure SW quality & CPSQ in your organization

Teams/projects
- Strive for high performance
- Use best practices & tools
- Define & track quality objectives
- Avoid arbitrary and unrealistic schedules or constraints

Individuals
- Learn and grow a disciplined approach
- Don’t be afraid of quality metrics
- Use existing knowledge sources of bug pattern and structural quality flaws

DevQualOps Concept Model